Monday, November 16	
9:00-9:45 am	*Keynote* **Ed Skoudis, Fellow, SANS Institute**
9:45-10:30 am	**Hacking Ugly: How Doing Things the "Wrong" Way Sometimes Turns out Right** We've all seen them: A smart and elegant hack that is - in its own way - a thing of beauty. This talk is not about those. While elegance and intelligence have their place, oftentimes brute force and ignorance win the day. While I can, at times, pull a little hacking elegance out of my hat, more often than not, I've found that knowing when "hacking purty" is a waste of time is the most useful tool you can have in your arsenal. I'll show you how "hacking ugly" can make you more productive, tell a few "war stories," and even pass on a few tricks that - if properly used - can make you look like a hacking god! **Tom Liston, Warner Brothers**
10:30-11:00 am	**Networking Break and Vendor Expo**
11:00-11:45 am	*Panel* **How I Detect Your Crappy Pen Test** *Session description to come* **Moderator: Ed Skoudis, Fellow, SANS Institute** **Panelists:** **Jorge Orchilles, Author, *Microsoft Windows 7 Administrator's Reference*** *Additional panelists to be named*
11:45am-12:15 pm	*Session to be Announced* **Kevin Finisterre**
12:15-1:30 pm	**Lunch**
1:30-2:15 pm	**What Goes In, Must Come Out: Egress-Assess and Data Exfiltration** Abstract: Every organization faces the possibility of being hacked, and it's a good idea to adopt Microsoft's "assume breach" mentality. It's important to note that most hackers today aren't in it for the lulz, but are in it to steal data. Organizations are constantly facing targeted attacks by motivated attackers due to the data they've accumulated over time. Attackers can leverage this data, if stolen, for identity fraud or other nefarious purposes. The white-hat industry needs to emulate today's threats to better prepare our customers for the actions of attackers. Egress-Assess allows users to exfiltrating

	sensitive faux (PII, credit cards, etc.), and real, data out of their network to an endpoint they control over a variety of protocols. This capability can be used by both blue and red teamers to really test if their organization can detect and remediate sensitive data leaving their network boundaries. Additionally, while detecting data leaving the network is important, an ideal world would allow defenders to catch malware or malicious groups before data exfiltration can take place. Egress-Assess is gaining the ability to emulate known malware, and will use documented indicators to simulate malware. This new feature will allow defenders and pen testers to better emulate documented threats and test if network defenses can catch malware operating in their environment. **Chris Truncer & Steve Borosh, Red Teamers**
2:15-3:00 pm	*Title & Session Description to come* **Raphael Mudge, Founder & Principal, Strategic Cyber LLC**
3:00-3:30 pm	**Networking Break and Vendor Expo**
3:30-4:15 pm	**DIY Vulnerability Discovery with DLL Side Loading** In this talk, Jake will teach you how to discover vulnerabilities like a rock star using DLL side loading. This technique (ab)uses the way Windows searches for DLLs to load into a program. The behavior is nearly laughable and introduces serious risks, especially when developers don't understand filesystem permissions. Attackers know this and use it for privilege escalation and stealthy persistence. It is being seen in a number of APT compromises and antivirus software has abysmal detection rates. **Jake Williams, Rendition Infosec**
4:15-5:00 pm	**Building an Empire with PowerShell** Offensive PowerShell had a watershed year in 2014. But despite the multitude of useful projects, many pentesters still struggle to integrate PowerShell into their engagements in a secure manner. The Empire project aims to solve the weaponization problem by providing a robust PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework. This is the post-exploitation agent you've been waiting for. **Will Schroeder, Project Lead, Veris Group** **Justin Warner, Project Lead, Veris Group**
Tuesday, November 17	
9:00-9:45 am	*Title & Description to Come* **Matt Carpenter, Principal Security Researcher, Grimm**

9:45-10:30 am	*Title & Session Description to come* **John Strand, Black Hills Information Security**
10:30-11:00 am	**Networking Break and Vendor Expo**
11:00-11:45 am	**Evil DNS Tricks** DNS is a weird and fantastic protocol that lets any system on even the most secure networks talk to an evil system (aka me) without ever sending it a packet. Who wouldn't love that? Every pen tester needs to know how to leverage the DNS infrastructure to find vulnerabilities, exploit vulnerabilities, and even set up a discreet two-way channel. This talk will cover the latest weaponization of DNS - including the newly re-written dnscat - and a pile of other fun DNS tricks! **Ron Bowes, Security Engineer, Google**
11:45am-12:15 pm	**My password cracking brings all the hashes to the yard...** ..and they're like, it's better than yours. Damn right it's better than yours, but I can teach you, free of charge. Password cracking is serious business, from dictionaries, to word munging, to Amazon EC2 and massive GPU rigs. Yeah, that's a lot of stuff! When I started cracking passwords, I knew there had to be a better way then just straight brute force; quite frankly, I never had a complex password crack over 8 characters finish even with some GPUs. I started asking friends, Googling and all I ever got was technical advice on how to run a tool, but never a methodology. It seemed the methodology was either a secret or they had about as much clue as I did; little. In this talk I'll discuss the outcomes of all of my research AND the methodology for really effective password cracking that even my CFO will approve. I may not have all of the answers, but what answers I do have, I'm willing to share. **Larry Pesce, Senior Security Analyst, InGuardians**
12:15-1:30 pm	**Lunch**
1:30-2:15 pm	**IoT Devices Fall like Backward Capacitors (Or the Month Josh Was Forced to Wear Pants)** Over the summer, Josh took on a special project. The setup was straightforward: login to Amazon, and buy 5 popular Internet of Things (IoT) devices. The goal was also straightforward: build remote exploits for the devices, winning bug bounty money to sufficiently cover the cost of the project. In this talk, Josh will present his findings from his *Summer of IoT Hacking*, presenting the techniques used for attacking these embedded, purpose-built devices. He will also share the entertaining and heart-breaking experiences from working with vendors to claim bug bounty prizes, and how you can apply these techniques to expand your breadth of skills and knowledge in your next penetration test. **Josh Wright, Senior Technical Analyst, CounterHack**
2:15-3:00 pm	

	DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods. **Kevin Fiscus, Founder, Cyber Defense Advisors & Certified Instructor, SANS Institute**
3:00-3:20 pm	**Networking Break and Vendor Expo**
3:20-4:05 pm	*Title & Session Description to come* **Tim Medin, Senior Technical Analyst, CounterHack**
4:30-10:00 pm	**Hackfest Hits the Road** Join Ed Skoudis, Summit speakers and your fellow attendees for a very special off-site event. The details are top secret and will be revealed at the Summit, but it promises to be an unforgettable evening of education and networking. A light dinner and refreshments will be provided.