This is not the final version of the agenda! Please check back often as we add more great talks, and note that all times are subject to change.

Monday, November 18	
9:00-9:15 am	*Welcome & Opening Remarks*
9:15-10:00 am	*Keynote* **Raphael Mudge** @armitagehacker, President, SpectreOps, Inc.
10:05-10:40 am	**Trials and Tribulations of Modern Malware Control** **Jonathan Echavarria** @Und3rf10w, Offensive Security Engineer – Red Team, Facebook Modern malware utilizes a myriad of methods to transport control information between the operator and the malware itself. This talk will cover a review of the landscape of modern malware control mechanisms, the use of redirections and exfiltration methods, identify key points of detection and fingerprinting of various methods, and discuss options for implementing your own control mechanisms.
10:40-11:10 am	**Networking Break**
11:15-11:50 am	**The C2 Matrix: Comparing C2 Frameworks** **Jorge Orchilles** @jorgeorchilles, Certified Instructor, SANS Institute Come with me on a quest to compare and contrast C2 frameworks for Red Teaming and Threat-Led Penetration Testing. With so many options available, which one is the best choice for your current situation? I will present a C2 Comparison Matrix that will help you choose.
11:55 am – 12:30 pm	**Discovering Vulnerabilities Using IDA Scripting** **Stephen Sims,** @Steph3nSims, Fellow, The SANS Institute In this talk, we will walk through several examples of scripting with Interactive Disassembler (IDA) to discover vulnerabilities. We most often think of discovering bugs through the process of fuzzing, but understanding the inner workings of a

	bug class can enable you to find new bugs through static analysis and scripting. Similarly, this is also a benefit to performing binary diffing. If you determine how a type of vulnerability is patched at the assembly level, you can use that knowledge to identify the same vulnerability at other locations within the code.
12:30-1:30 pm	**Lunch**
1:35-2:10 pm	**Crazy Windows Privilege Escalation Tricks That Your Blue Team Hates** **Jake Williams** @malwarejake, President, Rendition Infosec In most enterprise environments, it's increasingly uncommon to find users logged in with local admin privileges. But escalating to at least a local admin is critical for a number of operations. In this talk, we'll demonstrate a number of tricks to elevate to local admin on Windows machines. We won't be talking about unpatched vulnerabilities – Nessus can find that for you. Instead, we'll focus on tricks that rely on misconfigurations commonly found in enterprise.
2:15-2:50 pm	**Maniacal Keyboards** **Kevin Tyers,** @waronshrugs, Head of Infrastructure, iCTF, SANS Instructor This talk will cover Human Interface Device (HID) attacks, focusing on keyboards. Fusing information security knowledge and mechanical keyboard enthusiasm, we will cover HID attack basics, devices, and defenses. The final portion of the presentation will cover building your own keyboard with a variety of HID attacks prebuilt and ready to deploy during an engagement.
2:50-3:15 pm	**Networking Break**
3:20-3:55 pm	**How to Train Your Dragon: Ghidra Basics** **Jaime Geiger** @jgeigerm, Computer Attitude Counselor, GRIMM What is Ghidra? Where is it going? How can it help you with your job? How is it impacting the reverse-engineering community and disassembler market? This presentation will answer these questions and more in 35 minutes or less!
4:00-4:35 pm	**Pen Testing ICS and Other Highly Restricted Environments** **Don C. Weber** @cutaway, Principal Consultant, Founder, Cutaway Security, LLC, Instructor, SANS Institute

	"Congratulations, you have been selected to conduct a penetration test of our industrial control system (ICS) environment. Please remember, you cannot scan anything, you cannot install anything, and you cannot break anything. Your point of contact, who will watch every move you make, will be..." This is not a joke. More and more companies are requesting penetration tests of their ICS assets. But how can you conduct testing with these restrictions and provide actionable information to secure the customer's environments? This presentation will discuss how to scope and conduct this type of assessment. Attendees will walk away with the skills needed to safely evaluate critical networks and assets and make the customer's team comfortable about the assessment.
5:30-???	**HackFest FunFest** As always, we'll whisk you away to an off-site destination for networking, a custom Counterhack Challenge, and, OF COURSE, JoMama's cookies. Details are on a need-to-know-basis.
Tuesday, November 19	
9:00-9:45 am	*Keynote*
9:50-10:25 am	**Covert Channels & Command and Control Innovation** **Rilke Petrosky Ulloa**, @xenomuta, Red Team Leader and Security Researcher, F2TC Cyber Security Defensive technologies and innovation out-weights those of its offensive counterpart, increasingly draining red teamers out of options in every exercise, as the blue team achieves a higher maturity level by implement better and more tool-centric controls. Remaining stealth is becoming more of a challenge, forcing the red team to become innovative as one would expect from real threat actors. Broaden your perspective by attending this talk where we will present creative and unexpected techniques and procedures for practical red teaming that adapts to scenario-specific cases. In this talk we will cover the following topics that will help you better emulate an advanced adversary: • Shift into the mindset of sophisticated adversary. • Get inspired into unexplored options that hide in plain sight. • Thwart next-generation Antivirus and AI/ML-based EDRs solutions. • Learn inspiring and unexpected (ab)uses of already existing resources. • Dwell behind enemy lines undetected by achieving objectives while blending your operation with expected user behavior.

	Speaker: Rilke Petrosky Ulloa, Red Team Leader and Security Researcher, F2TC Cyber Security
10:25-10:55 am	**Networking Break**
11:00-11:35 am	**Using Mobile Malware Tactics During Penetration Tests** **Jeroen Beckers**, NVISO Techniques used by penetration testers are often used by malware and vice versa, either to get initial access to the target system, pivot inside the network or escalate privileges. Mobile devices also have their share of malware, but the techniques they use are rarely applied in actual penetration tests. In this talk, I will show you different kinds of Android malware, explain how they abuse the Android ecosystem and examine if these techniques can be used during penetration tests.
11:40 am – 12:15 pm	**Introduction to Modern Heap Exploitation for Penetration Testers** **Huáscar Tejeda** @htejeda, Co-Founder and CEO, F2TC Cyber Security Operating systems have considerably hardened stack memory corruption vectors to a point that finding stack vulnerabilities in modern software packages is very unlikely. Take your penetration testing engagements to the next level by harnessing the often unexplored advantages of heap exploitation. In this talk you will learn the following game-changing skills that will help you identify otherwise obscure attack vectors: • Understand high-level Linux dynamic memory allocation concepts. • Develop the intuition to identify exploitation opportunities in the way developers manage dynamic memory. • Pro-tips for setting a debugging/research lab. • Save time by evading rabbit-holes and complexities of studying heap exploitation. • Overview of different heap exploitation techniques. • Walkthrough real-life (ab)use cases.
12:15-1:15 pm	**Lunch**
1:20-1:55 pm	*Talk to be announced*
2:00-2:35 pm	*Talk to be announced*

2:35-3:00 pm	**Networking Break**
3:05-3:40 pm	*Talk to be announced*
3:45-4:20 pm	*Talk to be announced*
4:25-5:00 pm	*Talk to be announced*
5:00-5:15 pm	*Wrap-Up*

Speaker Biographies

Jeroen is the mobile security lead at NVISO where he is responsible for quality assurance on mobile security projects and for R&D on all things mobile. He started working on Android security in his Master's thesis and now has more than 5 years of experience in mobile security. He loves sharing his knowledge with other people, as is demonstrated by his many talks & trainings at colleges, universities, clients and conferences. Jeroen is also a co-author of the OWASP Mobile Security Testing Guide (MSTG) and Mobile Application Security Verification Standard (MASVS).

Jonathan Echavarria @Und3rf10w, Offensive Security Engineer – Red Team, Facebook
is an offensive security engineer on Facebook's Red Team where he conducts a variety of operations targeting Facebook as an organization. Previously, Jonathan worked at a startup doing everything from penetration testing, red teaming, devops, automation, building a SOC, and security architecture for a little over 6 years. He's also spoken at a number of conferences on topics such as cybercrime, state-sponsored operations, and smart home security. When not working, you can find Jonathan carving through canyon roads, tinkering with various home automation devices, or listening to music.

Jaime Geiger @jgeigerm, Computer Attitude Counselor, GRIMM is an experienced forward and reverse engineer with a passion for teaching. In addition to teaching for SANS, he currently works in the Washington DC area for Grimm, where he enjoys the freedom to work on software design and implementation, reverse engineering, exploit development, and network administration.

Raphael Mudge @armitagehacker, President, SpectreOps, Inc.
Raphael is the founder and president of SpecterOps, Inc. Raphael is also the Principal at Strategic Cyber LLC, the firm that develops the Cobalt Strike platform for Adversary Simulations and Red Team Operations. Previously, Raphael worked on red team automation through DARPA's Cyber Fast Track program. Today, Raphael speaks on security topics and provides volunteer red team support to many student cyber defense exercises. Raphael is a U.S. Air Force veteran.

Jorge Orchilles @jorgeorchilles, Certified Instructor, SANS Institute
Jorge founded The Business Strategy Partners in 2002 to provide consulting services to residential and small businesses, then founded Florida International University's MIS Club and was contracted to work on the university's Active Directory Migration Project. In 2007 he joined Terremark, a datacenter and cloud service provider acquired by Verizon. He helped build and secure Terremark's Infrastructure as a Service solution and was promoted to a Security Operations Center analyst in 2009 before moving on to an offensive analyst position with a global financial institution. Jorge has performed hundreds of application and infrastructure vulnerability assessments and penetration tests, and has led numerous teams of ethical hackers.

Kevin Tyers, @waronshrugs, Head of Infrastructure, iCTF, is a SANS Instructor who teaches SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling. He is also the head of cyber intelligence engineering for a Fortune 250 company, and the head of infrastructure for iCTF. Kevin holds the GCIH, GPEN, GCIA, GNFA, GCWN, and GCUX certifications. He is the cofounder of the Information Security group DC480 in Phoenix, Arizona.

Jake Williams @malwarejake, President, Rendition Infosec is the founder and President of Rendition Infosec, where he performs red team, digital forensics, and incident response operations. Prior to founding Rendition, he worked for the U.S. government in various information security roles. Jake enjoys making technical topics accessible to and actionable by decision-makers.