SANS The most trusted source for cybersecurity training, certifications, degrees, and research

PENTEST HACKFEST

Program Guide

@SANSPenTest
#SANSHackFest

Agenda

All Summit Sessions will be held in the Regency Ballroom, Ballroom Level (unless noted otherwise).
All approved presentations will be available online following the Summit at ***sans.org/summit-archives***

Monday, November 18

7:00-9:00 am	**Registration & Coffee** (LOCATION: REGENCY FOYER)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Stephen Sims*** *@Steph3nSims, Summit Co-Chair, SANS Institute* ***Ed Skoudis*** *@edskoudis, Summit Co-Chair, SANS Institute*
9:15-10:00 am	***Untitled Keynote, 2019*** Raphael Mudge is back on the keynote stage after a brief HackFest hiatus. Will he share his thoughts on the future of red teaming? Will he release a tool? Will he give out his closely-guarded recipe for his famous Thanksgivin' Stuffin' Muffins? There's no telling, but, in any case, you won't want to miss it. ***Raphael Mudge*** *@armitagehacker, Principal, Strategic Cyber LLC*
10:05-10:40 am	***Trials and Tribulations of Modern Malware Control*** 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. ***Jonathan Echavarria*** *@Und3rf10w, Offensive Security Engineer – Red Team, Facebook*
10:40-11:10 am	**Networking Break** (LOCATION: REGENCY FOYER)
11:15-11:50 am	***What Every Pen Tester Needs to Know About ICS*** Industrial Control Systems hold multiple connotations for penetration testers. On the one hand, there's a presumption that they'll be out-of-date, neglected, and easy targets. On the other hand, they are often considered fragile, untouchable, and incomprehensible. This talk delves into the myths and realities of ICS today, as well as the practicalities of evaluating and securing them. Initiating conversations with Operational Technology (OT) teams will be discussed, as well as ways to expand knowledge about ICS in several industry verticals. ***Lesley Carhart*** *@hacks4pancakes, Principal Threat Analyst - Threat Operations Center, Dragos, Inc.*
11:55 am – 12:30 pm	***How to Train Your Dragon: Ghidra Basics*** 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! ***Jaime Geiger*** *@jgeigerm, Computer Attitude Counselor, GRIMM*
12:30-1:30 pm	**Lunch** (LOCATION: REGENCY FOYER)

Monday, November 18

1:35-2:10 pm	***Crazy Windows Privilege Escalation Tricks That Your Blue Team Hates*** 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. ***Jake Williams*** *@malwarejake, President, Rendition Infosec*
2:15-2:50 pm	***Maniacal Keyboards*** 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. ***Kevin Tyers*** *@waronshrugs, Head of Infrastructure, iCTF, SANS Instructor*
2:50-3:15 pm	**Networking Break** (LOCATION: REGENCY FOYER)
3:20-3:55 pm	***Break it 'Til You Make It: How Playing with Fire Levels Up Your Offensive Skills*** All work and no play make dull pen testers. But we're so busy, we often fail to make time for play. Time to shift your thinking. Get away from the keyboard and break something, burn something, or build something. Feel like a waste of time? It's NOT. Learn how hands-on puttering can make you a better red teamer. MODERATOR: ***Ed Skoudis*** *@edskoudis, Summit Co-Chair, SANS Institute* PANELISTS: ***Stephen Sims*** *@Steph3nSims, Summit Co-Chair, SANS Institute* ***Kevin Tyers*** *@waronshrugs, Head of Infrastructure, iCTF, SANS Instructor* ***Don C. Weber*** *@cutaway, Principal Consultant, Founder, Cutaway Security, LLC, Instructor, SANS Institute*
4:00-6:00 pm	***SANS Pen Test Hardware Hacking Village: Intro to Soldering*** LOCATION: CABINET/JUDICIARY Sparks will fly in this hands-on workshop. Were you one of those kids who dismantled household electronics for fun? Come learn the first step to hardware hacking by learning to solder. You'll get hands-on experience to start on your way to building controllers and hacking boards. ***Micah Hoffman*** *@WebBreacher, SANS Institute*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Tuesday, November 19

7:00-9:00 am	**Registration & Coffee** (LOCATION: REGENCY FOYER)
9:00-9:45 am	***Keynote: Attacking and Defending the Microsoft Cloud (Office 365 & Azure AD)*** The allure of the "Cloud" is indisputable. Organizations are moving into the cloud at a rapid pace. Even companies that have said no to the Cloud in the past have started migrating services and resources. The Cloud is a new paradigm and the rapid update pace makes it difficult to keep up, especially when it comes to security. This presentation focuses on the Microsoft Cloud (Office 365 & Azure AD) and explores the most common attacks against the Cloud and describes effective defenses and mitigation. While the content is focused on the Microsoft Cloud, some of the attack and defense topics are applicable to other cloud providers and are noted where applicable. ***Sean Metcalf*** *@PyroTek3, CTO, Trimarc* ***Mark Morowczynski*** *@markmorow, Principal Program Manager, Microsoft*
9:50-10:25 am	***Covert Channels & Command and Control Innovation*** Defensive technologies and innovation out-weights those of its offensive counterpart, increasingly draining the red team out of options in every exercise, as the blue team achieves a higher maturity level by implementing 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 ***Rilke Petrosky Ulloa*** *@xenomuta, Red Team Leader and Security Researcher, F2TC Cyber Security*
10:25-10:55 am	**Networking Break** (LOCATION: REGENCY FOYER)
11:00-11:35 am	***Using Mobile Malware Tactics During Penetration Tests*** 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. ***Jeroen Beckers****, NVISO*

Tuesday, November 19

11:40 am – 12:15 pm	***Introduction to Modern Heap Exploitation for Penetration Testers*** 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. ***Huáscar Tejeda*** *@htejeda, Co-Founder and CEO, F2TC Cyber Security*
12:15-1:15 pm	**Lunch** (LOCATION: CABINET/JUDICIARY) ***Leveraging Graph Databases to Find Zero Days & Business Logic Flaws*** This technical lunch & learn, will teach application security professionals how to query a semantic graphical representation of their source code to identify business logic flaws and zero day vulnerabilities including: data leakage, rootkits, backdoors, logic bombs, sql injection, cookie injection and XXE. Many of these vulnerabilities cannot be found by traditional code analysis tools, which rely on pattern-matching, because traditional code analysis has no insight into unique business logic or custom sanitization steps. However, new graph-based approaches, that combine the security analyst's knowledge with powerful query languages, are helping identify zero-day vulnerabilities 10-20X faster than manual review. ***John McDonald****, Director of Engineering, ShiftLeft, Inc.*
1:20-1:55 pm	***#TheC2Matrix: Comparing C2 Frameworks*** 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. ***Jorge Orchilles*** *@jorgeorchilles, Certified Instructor, SANS Institute*
2:00-2:35 pm	***Sneaky Tips and Tricks with Alternate Data Streams*** Alternate Data Streams are little known to most Windows (and Mac) power users and can easily be leveraged as sneaky places to hide executable code and scripts. Most administrators don't know about them and most AV's can't scan them – especially when hidden in strange places like File System reserved directories! Come learn about the wonderfully strange ways we can hide and execute code from this often-overlooked oddity with several demos! ***Sean Pierce****, Red Team Lead, Target*
2:35-3:00 pm	**Networking Break** (LOCATION: REGENCY FOYER)

Tuesday, November 19

3:05-3:40 pm	***Discovering Vulnerabilities Using IDA Scripting*** 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. ***Stephen Sims*** *@Steph3nSims, Fellow, The SANS Institute*
3:45-4:20 pm	***Pen Testing ICS and Other Highly Restricted Environments*** "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. ***Don C. Weber*** *@cutaway, Principal Consultant, Founder, Cutaway Security, LLC, Instructor, SANS Institute*
5:00-8:30 pm	**HackFest Night Out** The FBI Experience: We have a super exciting night planned for our Pen Test HackFest Summit attendees. We are going on a field trip to the FBI Headquarters in Washington, DC.
6:30-9:30 pm	**Core NetWars** (LOCATION: CABINET/JUDICIARY) Prefer to skip the field trip and hunker down for CTF-style action instead? You're in luck. Core NetWars Tournament 6 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. Laptop Requirements: A laptop capable of running a VMware virtual machine, with a USB port and connecting to an Ethernet network is required.

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.