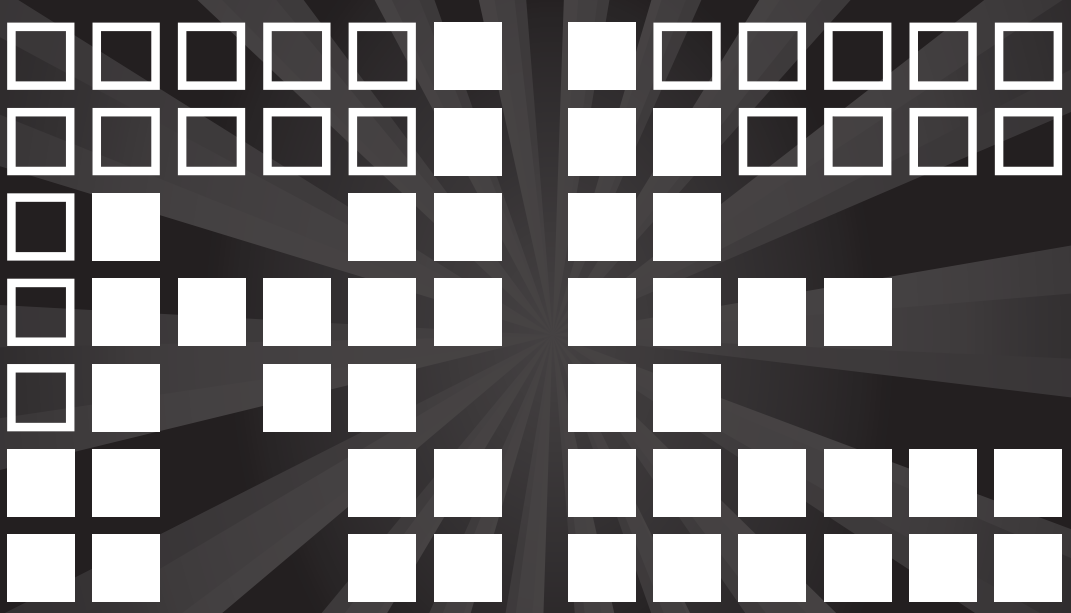
PROGRAM 2016

DERBYCON 6.0



CHARGE

LOUISVILLE, KENTUCKY • 2016

9.23.2016 - 9.25.2016

We made it! Welcome to DerbyCon 6.0 “ReCharge”.

This year’s theme was picked because of how we feel each year we come to DerbyCon. Walking in the Hyatt and smelling the air, the prep work it takes to get to an actual conference, and most importantly, meeting our extended family. We leave DerbyCon recharged and ready to take on the issues that face the security industry. For those that are new to DerbyCon, this conference is designed with our values, that values that you are welcome regardless of your past, present, or future. Everyone here is on equal playing fields and approachable. Our goal is to learn from one another and share our experiences because everyone provides value to making the INFOSEC industry better. For those that have been here since DerbyCon 1.0, we appreciate your commitment and can’t wait to see you again. For us, DerbyCon is more than a conference, it’s a time for us to get together, share ideas, and to meet one another and learn. Over the years, we have not only met new individuals to INFOSEC, but had the opportunity to see them grow and become awesome and contributing folks to the INFOSEC community.

A good example is a great friend of ours named Jason Ashton. Jason was a sound engineer and wanted to make a career change, working on the side learning INFOSEC and wanting to become a hacker. His drive and passion led him to DerbyCon. He happened to see Martin Bos on Twitter ask if anyone was good at being a sound engineer and wanted to volunteer for help. Jason messaged Martin and from there his career skyrocketed in INFOSEC. Jason is now a senior security consultant and one of the core folks that help us get the DerbyCon parties going with sound, and he’s one heck of a consultant. This is what DerbyCon is about. Recognizing that people from all places in their career from the beginning and to the end are part of the conference. You are truly what makes the conference what it is.

A story that is one of the most memorable: A tweet from DerbyCon 1.0 where someone new to INFOSEC who had followed Kevin Mitnick since they were a kid posted: “I’m at a bar and Kevin Mitnick just came up to us and bought us a drink and hung out with us for the night! THIS IS AMAZING”. Another story: Last year going to the Third Street dive bar and seeing the entire bar packed with DerbyCon folks, socializing, removing barriers - something that tends to be difficult for us socially. Dual Core getting up on stage at the bar and free styling (hack all the things).

There are countless stories of relationships made, careers started, and lifelong friendships crafted. This conference is for the industry because you deserve it. We have some of the most talented and brilliant people that has ever been on this Earth. Thank you for making DerbyCon what it is, and have one heck of a time.

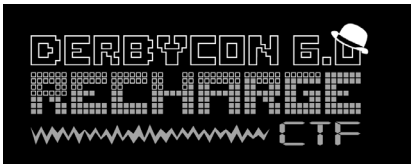
Remember to be respectful of one another, recognize personal space, have an amazing time, and most importantly recharge yourself.

Welcome to DerbyCon 6.0 - ReCharge.

DerbyCon

Registration times: Friday - 8am to 11am, 12pm to 3pm, 6pm to 8pm,
Saturday - 8am to 12pm, Sunday - T-shirt booth
Located on 2nd floor outside of the conference theater

ALL WEEKEND EVENTS – 9.23 - 9.25



Capture the Flag

Conference Theater & (Oaks room - 24 hr access available)
Conference Theater hours: Friday 12pm to 9pm
Saturday 9am to 9pm – Sunday 10am to 12pm

The capture the flag event is an open event and there are no qualifiers. Anyone can participate via self-registration. There will be posters around the venue with information on how to connect and play as well as information regularly distributed through the official DerbyCon CTF Twitter account @DerbyConCTF.

Wireless access will be available 24/7 so that participants can play even when the CTF room is closed. The wireless network information is:
SSID: DerbyCon-CTF
PASSWORD: DerbyCon-CTF

CTF mimics a penetration test in that you must enumerate systems, services, and find vulnerabilities and exposures to further access and find flags. Flags are worth different point values based mostly upon difficulty. A public scoreboard system will be used to track points real time. Prizes will be awarded to the first 10 places and winners must be present to claim their prize (only one prize per team).

Prizes are the following:

Black Badge	Sparrows The EOD
Free ticket to DC 7.0	LAN TAP PRO
Proxmark 3 RDV2 kit	$200 Amazon
Ubertooth One	$100 Amazon
ODroid-XU4	$50 Itunes

Scavenger Hunt:

Scavenger Hunt at DerbyCon RETURNS for 2016!!!

For the last two years, people have been dancing, rhyming, and eating dinner with mittens all in the name of winning! This year, there will be even more of the same wacky shenanigans. Are you unmotivated to get involved in all the complicated time consuming efforts in order to "participate" at conferences? Are you looking for a healthy outlet for all the weirdness you are suppressing? Ever wish you could win a contest without the hassle of having to miss talks, lobby con, or hugging people awkwardly? If you suffer from a compulsive need to witness and/or mastermind mild to moderate trolling, then we have the game for you! Scavenger Hunt 3.0 at Derby Con, presented by The Glue Factory.

Follow us on Twitter for signup and instructions
@TwatWaffleCrew

Car Hacking Village

Gulfstream & Hialeah rooms,
Friday and Saturday 10am to 7pm – Sunday 10am to 2pm

The Car Hacking Village is a Hand-On environment for understanding how vehicle systems work. Come join our village to sit down and play with vehicle controllers and understand how to get started in vehicle hacking. Join us to learn more about our upcoming Car Hacking CTF.

Lockpick Village:

Gulfstream & Hialeah rooms,
Friday and Saturday 10am to 7pm – Sunday 10am to 2pm

Come test your skills at the DerbyCon lockpicking village! From the absolute beginner to the old-hand, we have something for everyone. Try defusing "The Bomb" where you have to use skill and luck to stop the countdown before it goes critical! And go head-to-head with multiple lock pickers in the "Rumble Challenge" multi-round competition. Picking, bumping, high security locks, more games, and other surprises are waiting for you in the lockpicking village! Awesome schwag will be awarded for top places in all competitions. Come to learn, stay to compete!

Hardware Hacking Village

Gulfstream & Hialeah rooms,
Friday and Saturday 10am to 7pm – Sunday 10am to 2pm

LVL1, Louisville's Hackerspace, will be hosting a hardware hacking village, complete with devious and useful kits to solder together (no experience required! Through hole and surface mount kits available!), a 3D printer, along with a showcase of projects. Need some bling for the party? We'll have LED based kits to solder together, too. Interested in the low-level stuff? Stop by the hardware hacking village to hack together something of your own, chat with other hardware hackers, and check out some cool stuff. Interested in learning more about LVL1 and hackerspaces? Visit http://www.lvl1.org.

(Events continued on page 2-4)

SPECIAL EVENTS – 9.23 - 9.24

Hacker Jeopardy

Keeneland room, Friday 8pm (Arrive Early. Limited Seating. Beer Bribery, OK.)

DerbyCon Jeopardy Is Back!

(Oh, Hell Yeah, It Is!)

You know the game. You get publicly humiliated for saying stupid shit while chugging beers for a lousy 100 points a bottle! And the host and audience have all the fun. You know we will taunt you, abuse you and confuse you, for our merriment, of course.

Still Want to Play?

Submit your Team, up to 3 players each. Pick a name. Tell us why you think you're all that. Mobile contact info (private only). Oh! Yeah. Diversity counts!

Send your Team Submissions (and bribes) to: Winn@SecurityExperts.Com

Teams will be picked live at DerbyCon Jeopardy. So, that means, remember to Be There. (Oh, the abuse has already begun…)

Hack the Hat 2016 – Cycle OverRide's annual ride at DerbyCon

Saturday 7:30am – Meet in Hotel Lobby

Email info@cycleoverride.org if you plan on joining us.

The first year of DerbyCon, we actually cycled our way to the con from a few states away. The last few years we've simply opted to do a ride after arriving by more conventional methods. You're welcome. We're not entirely sure of the route yet, but we'll keep it under control with no major climbs (something Louisville lacks anyway). This will be a no-drop ride, but hopefully we can keep a decent speed and get around 20 miles in just over an hour. Ok. Maybe two. Hours. Not two miles. I digress.

It should be noted that we likely will NOT be back in time for the first talk, but almost certainly by the 2nd slot of the day. You are, of course, welcome to turn back early if necessary.

You're best bet for this ride is to bring your own bike if you can. Road or mountain or unicycle is fine – we're not breaking any records here. Unfortunately renting a decent bike in Louisville isn't as easy as we've found in other cities. There ARE places to rent and I'll update this page with some links after I make a phone call or two. We don't have enough critical mass for this ride to ask a shop to open up early however, so renting may require you to pick up your bike the day before. Again more details as I find them out. The good news is that Louisville is planning to set up bikeshare stations and while this did get delayed until 2016, maybe it will be in place for next year's ride.

BourbonCon

Hyatt – The Spire Rooftop Lounge, Saturday 9pm to Midnight

We return for our sixth year with a new location. BourbonCon is a bourbon tasting and social event. This years event is being held at the DerbyCon hotel in The Spire Rooftop event space. Admission this year is $30 cash only at the door, and pre-sales tickets are available via EventBrite for $40 (https://www.eventbrite.com/e/bourboncon-2016-tickets-26743147474) for those who want to make purchases via credit card. You can follow @bourboncon for updates leading up to the event and for any future event details. As in past years, we are taking any money beyond the operating cost of the event and donating it to charity. This year the money will be going to cancer research.

Belmont room

Friday

12pm to 2pm Sign Ups.
2:30pm to 6pm - Can you fool the lie detector?

"Can you fool the lie detector?" Is an original contest made just for DerbyCon. The Social-Engineer crew hires a world renowned Polygrapher to come to Derby and give LIVE, PUBLIC Polygraphs. You will be asked a series of super embarrassing questions and the goal is to tell the truth (or not) but to never let the Polygraph Machine or Polygraph Operator catch you!

Do you have the skill? If you do, the winner will be granted a FREE pass for next years DerbyCon, a Free SE Challenge Coin and some awesome SE Schwag.

Saturday

9:30am to 11am – Sign Ups
11am to 12:30pm and 1:30pm to 6pm

"Mission SE Impossible" or MSI has been revamped, improved and Derby-ized. Can you escape handcuffs? Pick Locks? Traverse Lasers? Solve Book Codes? Crack a Safe? All with a crowd watching, Chris breathing on you and the stress of a timer? Find out by taking part in the first ever MSI at DerbyCon.

Winners will get a DerbyCon 7.0 Pass, SE Challenge Coin and some awesome SE Schwag.

SPECIAL EVENTS – 9.23 - 9.24

SOHOpelessly Broken

Derby room, Friday 11am to 7pm
Saturday 11am to 7pm

SOHOpelessly Broken, presented by Independent Security Evaluators (ISE), is back at DerbyCon for our third year! We have expanded the contest to not only include SOHO routers, but other types of IoT devices such as network storage systems, cameras, and IP enabled toys!

Track 1: This is an at-con capture the flag style contest where contestants will be pitted against 15+ off-the-shelf IoT devices, hardened, but with known vulnerabilities. Contestants must identify weaknesses and exploit these devices to gain control. Pop as many as you can over the weekend to win.

Track 2: This is a surprise contest that will take place at random times throughout the conference.

Track 3: Hack shop area for people to actively hack and collaborate on selected devices.

Track 4: A variety of workshops and talks will be delivered throughout the weekend.

Hack Your Derby

All submissions must be displayed to the judges by 8pm on Saturday in the lobby and scoring will be totaled and finalized by Closing Ceremonies on Sunday.

Hack Your Derby is a contest held annually at the DerbyCon hacker convention in Louisville, Kentucky. It is simple and straightforward: turn a derby hat -- already a fine piece of functional fashion -- into something more. Exactly how much more is up to you. Feel free to express your hacker spirit in the vein of technological or aesthetic development. There are points awarded by the judges in each of those categories, as well as accolades for overall originality.

You may either work on your derby creation before the conference or compete using exclusively what you can source in and around the con hotel during DerbyCon itself. Overall, however, the themes of "make something new, make something epic, make something awesome" are the order of the day. Prizes TBD, based on who donates what, but rest assured that there will be multiple winners in a variety of categories!

Curious.

Aqueduct room, Friday 1o57 am Start Time
Aqueduct room will used by Ham Radio (see below) on Saturday 1:00 PM to 3:00 PM.

DAMMIT, I'M MAD! TOO LONG IT'S BEEN SINCE I'VE COME ACROSS A CURIOUS CODE OR TWO. ARE WE NOT DRAWN ONWARD, WE FEW, DRAWN ONWARD TO NEW ERA? ALWAYS SEEKING THAT WHICH WITHSTANDS GOOGLING. DON'T NOD. LOOK INSTEAD FOR THE DERBY TALISMAN. BORROW OR ROB? KNOWLEDGE OF THE VENDOR AREA MAY BE HELPFUL HERE. GO, DELIVER A DARE, VILE DOG! THE FIRST FIFTY WILL BE REWARDED. NOW DO I REPAY A PERIOD WON? OF COURSE, FAR PAST THE CHALLENGE OF THE DERBY. DEVIL NEVER EVEN LIVED. UNTIL NOW EVERYTHING'S BEEN HIDDEN, CURIOUS, NO? NAME NOW ONE MAN. SECRET NAME, TO WIN THE GAME, FIND US.

@CURIOUS_CODES

HTTP://CURIOUS.CODES

Ham Radio Exams

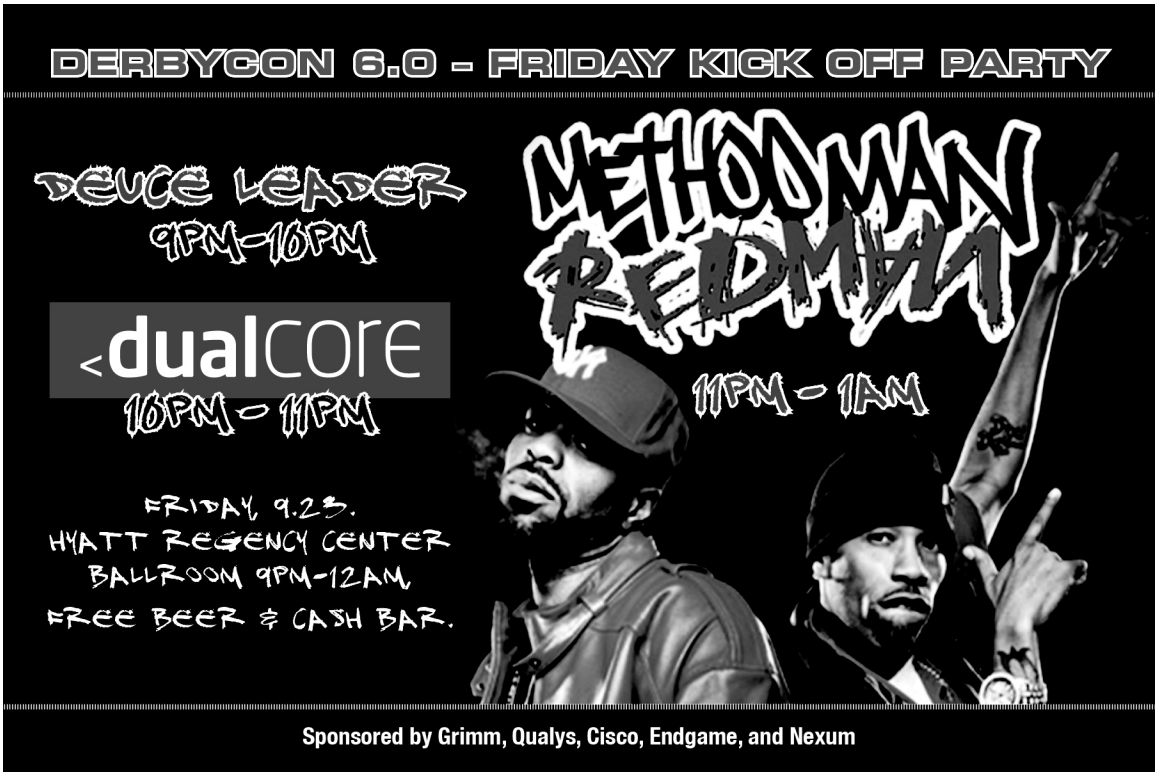
Aquaduct room, Saturday 1pm to 3pm – Exams
Sunday 1pm to 3pm – Retests

Amateur Radio (ham radio) is a popular hobby and service that brings people, electronics and communication together. People use ham radio to talk across town, around the world, or even into space, all without the Internet or cell phones. It's fun, social, educational, and can be a lifeline during times of need.

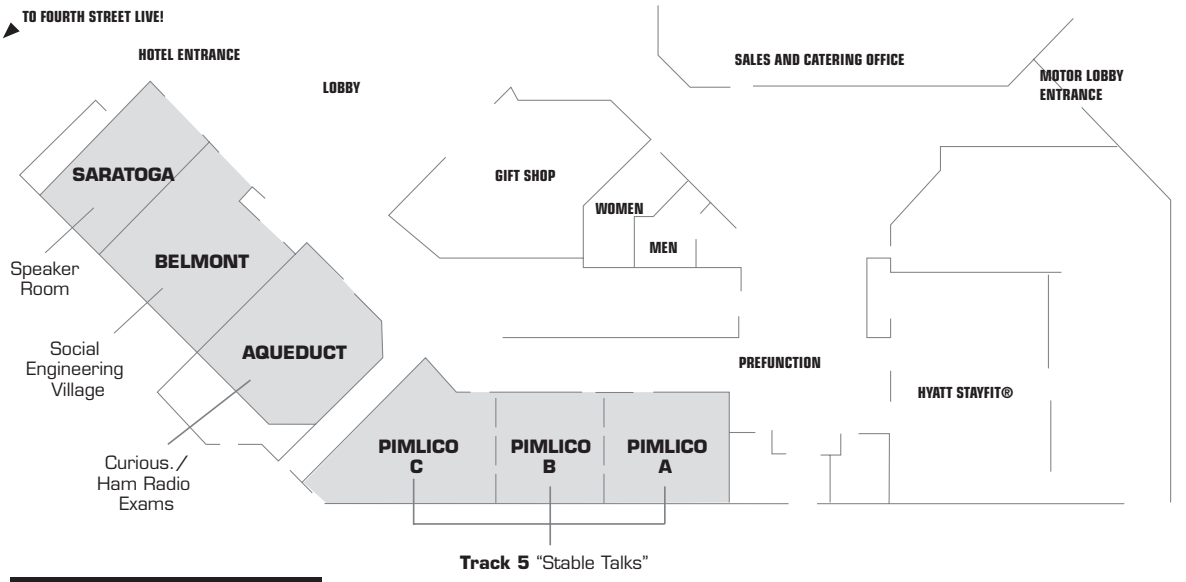
Returning to DerbyCon, will be the ham radio licensing exams! The cost is $15 (cash or check only). Check out the ARRL website for information on what to bring to the exam, as well as exam question pools, free study resources, and other FAQ.

No pre-registration is required.

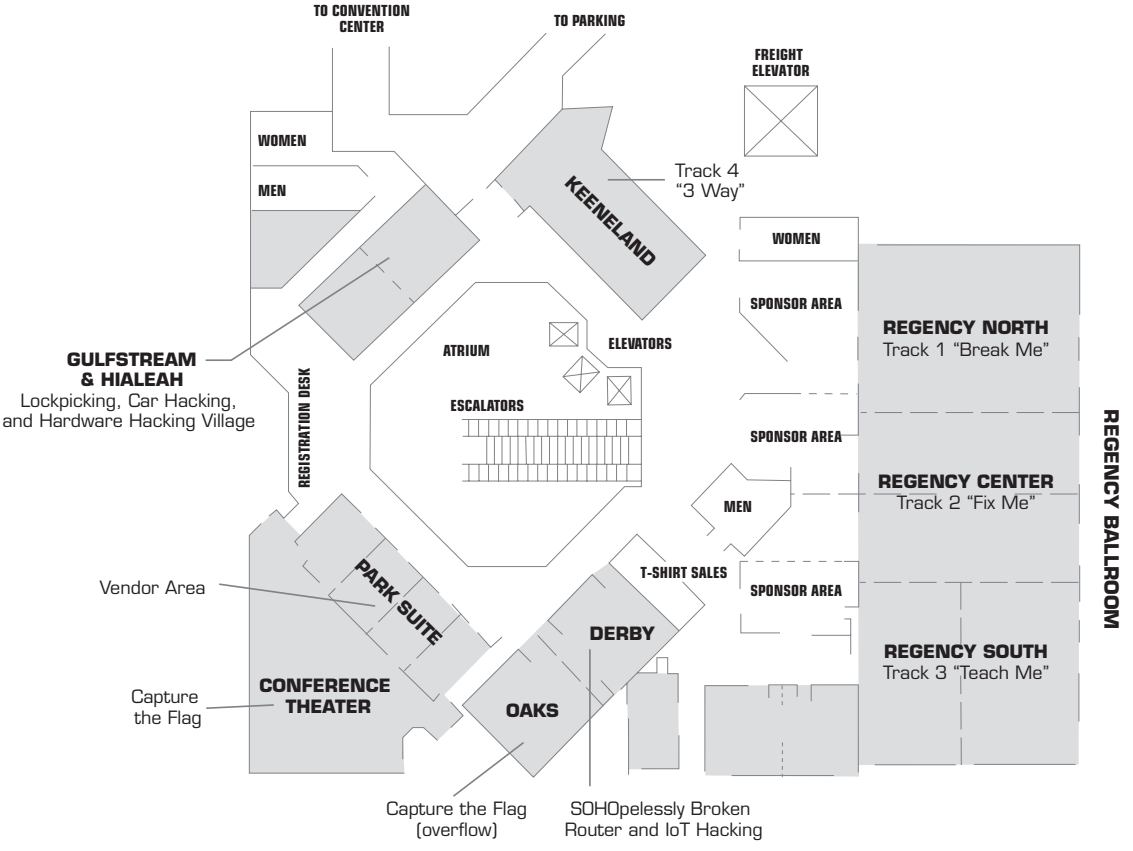
FRIDAY & SATURDAY PARTIES – 9.23 & 9.24



FIRST FLOOR



SECOND FLOOR



Training Courses 9.21 -9.22.
Safe Cracking: Mechanical and Electronic - Memory-Resident Code: Analysis, Detection, and Development - Advanced Exploit & Security - Advanced PowerShell for Blue and Red Teams - Advanced OSINT for Social Engineers - Application Security: For Hackers and Developers - Practical Web Application Penetration Testing (PWAPT) - Red Team vs. Blue Team - Pwning and Responding to SCADA Devices and Networks - Practical Network Signature Development for Open Source IDS - Tactical Sec Ops: Cloud Edition - AWS - Hack It and Track It - Pen Testing with Powershell - Introduction to Malware Analysis.

FRIDAY – 9.23. – Registration 8am to 11am, 12pm to 3pm, 6pm to 8pm

Friday Talk Descriptions Starts on Page 10

	Regency Ballroom
9:15am – 9:45am	**Opening Ceremonies –** DerbyCon Team
10:00am – 10:50am	**Keynote –** Jeffrey Snover, Lee Holmes
11:00am – 11:50am	Lunch

Talks	**Regency North Track 1 (Break Me)**	**Regency Center Track 2 (Fix Me)**	**Regency South Track 3 (Teach Me)**	**Keeneland Track 4 (The 3-Way)**
12:00pm - 12:50pm	Carlos Perez - Thinking Purple	Ed Skoudis - Internet of Things, Voice Control, AI, and Office Automation: BUILDING YOUR VERY OWN J.A.R.V.I.S.	David Maloney, James Lee, Brent Cook, Tod Beardsley, Lance Sanchez - Metasploit Townhall	Parker Schmitt - Data Obfuscation: How to hide data and payloads to make them "not exist" (in a mathematically optimal way)
1:00pm - 1:50pm	Mubix "Rob" Fuller - Writing malware while the blue team is staring at you	Christopher Hadnagy - Mind Reading for Fun and Profit using DISC	JDuck - Stagefright: An Android Exploitation Case Study	Arian J Evans & James Pleger - Top 10 2015-2016 compromise patterns observed & how to use non-traditional Internet datasets to detect & avoid them
2:00pm - 2:50pm	Tyler Halfpop , Jacob Soo - Macs Get Sick Too	Joe Desimone - Hunting for Exploit Kits	Stephen Breen, Chris Mallz - Rotten Potato - Privilege Escalation from Service Accounts to SYSTEM	Nick Cano - +1,000,000 -0: Cloning a Game Using Game Hacking and Terabytes of Data
3:00pm - 3:50pm	Will Schroeder, Matt Nelson - A Year in the Empire	Kevin Johnson and Jason Gillam - Next Gen Web Pen Testing: Handling modern applications in a penetration test	Ken Johnson, Chris Gates - DevOops Redux	Ryan Voloch and Peter Giannoutsos - To Catch a Penetration Tester: Top SIEM Use Cases
4:00pm - 4:50pm	BenOxA - PowerShell Secrets and Tactics	Michael Allen - Beyond The 'Cript: Practical iOS Reverse Engineering	Jayson E. Street - .... and bad mistakes I've made a few.....	Matthew Dunwoody, Nick Carr - No Easy Breach: Challenges and Lessons from an Epic Investigation
5:00pm - 5:50pm	Marcello Salvati - CrackMapExec - Owning Active Directory by using Active Directory	Rockie Brockway & Adam Hogan - Adaptation of the Security Sub-Culture	Zach Grace, Brian Genz - Better Network Defense Through Threat Injection and Hunting	nyxgeek - Hacking Lync (or, 'The Weakest Lync')
6:00pm - 6:50pm	Paul Coggin - Exploiting First Hop Protocols to Own the Network	Nick Landers - Outlook and Exchange for the Bad Guys	Valerie Thomas and Harry Regan - It's Never So Bad That It Can't Get Worse	Nathan Clark - AWSh*t. Pay-as-you-go Mobile Penetration Testing
7:00pm - 7:50pm	Mark Mager - Defeating The Latest Advances in Script Obfuscation	Concert Setup	Michael Gough - From Commodity to Advanced (APT) malware, are automated malware analysis sandboxes as useful as your own basic manual analysis?	

FRIDAY– 9.23. – Continued

Stable Talks	Pimlico A, B, C (Track 5)
12:00pm - 12:25pm	Jason Smith - Go with the Flow: Get Started with Flow Analysis Quickly and Cheaply
12:30pm -12:55pm	Devon Greene - Abusing RTF: Exploitation, Evasion and Exfiltration
1:00pm -1:25pm	Aaron Lafferty - Information Security Proposed Solutions Series - 1. Talent
1:30pm - 1:55pm	Alfredo Ramirez - DNSSUX: Why DNSSEC Makes Us Weaker
2:00pm - 2:25pm	wartortell and Aaron Bayles - Nose Breathing 101: A Guide to Infosec Interviewing
2:30pm - 2:55pm	William McLaughlin - Android Patchwork: Convincing Apps to Do What You Want Them To
3:00pm - 3:25pm	Spencer McIntyre - Is that a penguin in my Windows?
3:30pm - 3:55pm	Brent White && Tim Roberts - Real World Attacks VS Check-box Security
4:00pm - 4:25pm	Natalie Vanatta - ARRR Maties! A map to the legal hack-back
4:30pm - 4:55pm	Michael Wharton, Project MVP - Hacking and Protecting SharePoint
5:00pm - 5:25pm	Kevin Gennuso - Responder for Purple Teams
5:30pm - 5:55pm	Ken Toler - Metaprogramming in Ruby and doing it wrong.
6:00pm - 6:25pm	Nancy Snoke - Evolving your Office's Security Culture
6:30pm - 6:55pm	Michael Schearer - Confronting Obesity in Infosec
7:00pm - 7:25pm	Patrick Mathieu - BurpSmartBuster - A smart way to find hidden treasures
7:30pm - 7:55pm	Patrick DeSantis Joe Marshall, Carlos Pacho - Advanced Persistent Thirst (APT)

DERBYCON 6.0 FRIDAY KICK-OFF PARTY

Hyatt Regency Center Ballroom. 9pm to 1am, FREE BEER & Cash Bar.
Sponsored by Grimm, Qualys, Cisco, Endgame, and Nexum

SATURDAY – 9.24. – Reg. 8am to 12pm - after 12pm t-shirt booth

Saturday Talk Descriptions Starts on Page 15

Talks	Regency North Track 1 (Break Me)	Regency Center Track 2 (Fix Me)	Regency South Track 3 (Teach Me)	Keeneland Track 4 (The 3-Way)
9:00am - 9:50am	Tim MalcomVetter - Breaking Credit Card Tokenization Without Cryptanalysis	Bill V - Deploying PAWs as Part of a Strategy to Limit Credential Theft and Lateral Movement	Scott Lyons and Joshua Marpet - Business Developement: The best non-four letter dirty word in infosec.	Scot Berner, Jason Lang - Tool Drop 2.0 - Free As In Pizza
10:00am - 10:50am	Sean Metcalf & Will Schroeder - Attacking EvilCorp: Anatomy of a Corporate Hack	Matt Graeber - Living Off the Land 2: A Minimalist's Guide to Windows Defense	Kyle Wilhoit - Point of Sale Voyuer- Threat Actor Attribution Through POS Honeypots	Jeremy Mio, David Lauer, Mike Woolard - The Art of War, Attacking the Organization and Raising the Defense
11am-12pm	Lunch			
12:00pm - 12:50pm	Jay Beale - Phishing without Failure and Frustration	Larry Pesce - I don't give one IoTA: Introducing the Internet of Things Attack Methodology.	intOx80 (of Dual Core) - Anti-Forensics AF	Deral Heiland, Matthew Kienow - Managed to Mangled: Exploitation of Enterprise Network Management Systems
1:00pm - 1:50pm	egypt - New Shiny in Metasploit Framework	Jay Radcliffe - Five year checkup: the state of insulin pump security	John Strand - Penetration Testing Trends	Ellen Hartstack and Matthew Sullivan - Garbage in, garbage out: generating useful log data in complex environments

SATURDAY – 9.24. – Continued

Talks	Regency North Track 1 (Break Me)	Regency Center Track 2 (Fix Me)	Regency South Track 3 (Teach Me)	Keeneland Track 4 (The 3-Way)
2:00pm - 2:50pm	FuzzyNop - Embrace the Bogeyman: Tactical Fear Mongering for Those Who Penetrate	Eric Conrad - Introducing DeepBlueCLI, a PowerShell module for hunt teaming via Windows event logs	Dr. Jared DeMott & Mr. Josh Stroschein - Using Binary Ninja for Modern Malware Analysis	grid (aka Scott M) - Fuzzing basics…how to break software
3:00pm - 3:50pm	Jason Blanchard - How to Social Engineer your way into your dream job!	Lee Holmes - Attackers Hunt Sysadmins - It's time to fight back	Adam Compton, Austin Lane - Scripting Myself Out of a Job - Automating the Penetration Test with APT2	Branden Miller - Hacking for Homeschoolers: STEM projects for under $20
4:00pm - 4:50pm	David Schwartzberg and Chris Sistrunk - Make STEHM Great Again	Charles L. Yost - Python 3: It's Time	Philip Martin - DNS in Enterprise IR: Collection, Analysis and Response	Drew Branch - Need More Sleep? REST Could Help
5:00pm - 5:50pm	Bill Sempf - Breaking Android Apps for Fun and Profit	Amanda Berlin & Lee Brotherston - So You've Inherited a Security Department, Now What…	Brandon Young - Reverse engineering all the malware…and why you should stop.	Nathan Magniez - Body Hacking 101 (or a Healthy Lifestyle for Security Pros)
6:00pm - 6:50pm	Karl Fosaaen - Attacking ADFS Endpoints with PowerShell	Concert Setup	Stephen Hilt - The 90's called, they want their technology back	

Stable Talks	Pimlico A, B, C (Track 5)
9:00am - 9:25am	Joseph Tegg - We're a Shooting Gallery, Now What?
9:30am - 9:55am	Doug Burns - Malicious Office Doc Analysis for EVERYONE!
10:00am - 10:25am	Justin Herman & Anna-Jeannine Herman - Hacking though Popculture
10:30am - 10:55am	Josh Huff - Open Source Intelligence- What I learned by being an OSINT creeper
11:00am - 11:55am	Lunch
12:00pm - 12:25pm	Joey Maresca - Finding Your Balance
12:30pm -12:55pm	EvilMog - Hashcat State of the Union
1:00pm -1:25pm	Casey Smith - Establishing A Foothold With JavaScript
1:30pm - 1:55pm	Jesika McEvoy - Overcoming Imposter Syndrome (even if you're totally faking it)
2:00pm - 2:25pm	Craig Bowser - Security v. Ops: Bridging the Gap
2:30pm - 2:55pm	Chris "Lopi" Spehn - From Gaming to Hacking The Planet
3:00pm - 3:25pm	Scott Sutherland - SQL Server Hacking on Scale using PowerShell
3:30pm - 3:55pm	Brian Marks, Andrea Sancho Silgado - Dive into DSL: Digital Response Analysis with Elasticsearch
4:00pm - 4:25pm	Bill Gardner - Making Our Profession More Professional
4:30pm - 4:55pm	***Abe Miller*** - How are tickets paid for?
5:00pm - 5:25pm	Jimmy Byrd - Security Automation in your Continuous Integration Pipeline
5:30pm - 5:55pm	Chad M. Dewey - Cruise Ship Security OR Hacking the High Seas
6:00pm - 6:25pm	Lee Neely - Web Security for Dummies
6:30pm - 6:55pm	Kirk Hayes - I Love myBFF (Brute Force Framework)
7:00pm - 7:25pm	Cameron Craig, Keith Conway - Nobody gets fired by choosing IBM… but maybe they should.
7:30pm - 7:55pm	Mirovengi - Shackles, Shims, and Shivs - Understanding Bypass Techniques

DERBYCON 6.0 SATURDAY PARTY

Hyatt Regency Center Ballroom.Doors Open at 9pm. FREE BEER. Free Drinks with tokens.
Sponsored by SALESFORCE, MAIL CHIMP, SDGBLUE, RISKIQ, NCC GROUP.

SUNDAY – 9.25. – Registration T-shirt booth

Sunday Talk Descriptions Starts on Page 23

Talks	Regency North Track 1 (Break Me)	Regency Center Track 2 (Fix Me)	Regency South Track 3 (Teach Me)	Keeneland Track 4 (The 3-Way)
10:00am - 10:50am	Jared Haight - Introducing PowerShell into your Arsenal with PS>Attack	James Jardine - Recharging Penetration Testing to Maximize Value	hypervista - Poetically Opaque (or other John Updike Quotes)	David Boyd - Hack Yourself: Building A Pentesting Lab
11:00am - 11:50am	Andrew Krug Alex McCormack - Hardening AWS Environments and Automating Incident Response for AWS Compromises	Andrew Plunkett - Yara Rule QA: Can't I Write Code to do This for Me?	Anthony Kasza - Java RATS: Not even your Macs are safe	Beau Bullock, Derek Banks, Joff Thyer - The Advanced Persistent Pentester (All Your Networks Are Belong 2 Us)
12:00pm - 12:50pm	Daniel Bohannon - Invoke-Obfuscation: PowerShell obFUsk8tion Techniques & How To (Try To) D""e`Tec`T 'Th'+'em'	Dav Wilson - Mobile Device Forensics	Casey Cammilleri & Hans Lakhan - Hashview, a new tool aimed to improve your password cracking endeavors.	Brian Fehrman - Hardware Hacking the Easyware Way
1:00pm - 1:50pm	Ben Stillman - MariaDB: Lock it down like a chastity belt	Aaron Guzman - IoT Defenses - Software, Hardware, Wireless and Cloud	Adam Cammack, Brent Cook - Static PIE: How and Why	Braden Hollembaek, Adam Pond - Finding a Weak Link: Attacking Windows OEM Kernel Drivers
2:00pm - 2:30pm	Closing Ceremony Setup			
2:30pm - 3:30pm	**Closing Ceremony**			

Stable Talks	Pimlico A, B, C (Track 5)
10:00am - 10:25am	Ronnie Flathers - Abusing Linux Trust Relationships: Authentication Back Alleys and Forgotten Features
10:30am - 10:55am	Salvador Mendoza - Samsung Pay: Tokenized Numbers, Flaws and Issues
11:00am- 11:25am	Russell Butturini - Fire Away! Sinking the Next Gen Firewall
12:00pm - 12:25pm	Matthew Lichtenberger - PacketKO - Data Exfiltration Via Port Knocking
12:30pm -12:55pm	Jamie Murdock - Ransomware: An overview
1:00pm -1:25pm	Dan Bougere - The Beginner's Guide to ICS: How to Never Sleep Soundly Again

Please note that Derbycon.com will be the main source for important DerbyCon information and cancellations of talks and events. Follow @DerbyCon and #DerbyCon on Twitter.

FRIDAY – 9.23.

10:00am–10:50am KEYNOTE

Jeffrey Snover - @jsnover and Lee Holmes - @Lee_Holmes **– Vulnerability disclosure, cloudy clouds, and million dollar shopping trips. This industry sucks. And is awesome.**

Our beloved security industry is a complicated beast. Companies are collaborating with researchers more now than they have ever, but it's still easy to walk away feeling frustrated by an encounter with an otherwise seemingly responsive vendor. Microsoft's Technical Fellow Jeffrey Snover and Security Architect Lee Holmes share their unique perspectives on this relationship and shed some light the corporate behaviors that might otherwise feel out of touch, and share their perspectives on getting on a solid path to more secure systems.

This collaboration is making the world a safer place, however, and we now find ourselves at the cusp of another major industry shift. What does security look like in a world that's becoming increasingly cloud-connected? With the vast majority of cloud capacity coming from two companies in Seattle, what chance do you possibly have to keep yourself secure?

In addition to the torrid pace of change in our industry, there's still a lot of regular ol' security going on. New threats, new exploits, an ever changing attack surface. How do you keep YOUR companies secure in a world like this? It's tempting to throw your hands up, get a money order for a million dollars, and just go shopping at RSA. That may eventually be part of the solution but it rarely the most effective path forward. So what is?

12:00pm–12:50pm

Thinking Purple – ***Carlos Perez - @carlos_perez***

Breaking with the adversarial approach of Red vs Blue, look at how the current system and approaches may be broken in some organizations and provide recommendation not only for the mature organization with a large structure but also how small businesses can take a more purple strategy in the way they operate their teams including how they acquire pentest services. Presentation will cover an approach beyond the red and blue team and more of a organizational and strategic approach to change the paradigm of thinking and action to more symbiotic approach to security.

Internet of Things, Voice Control, AI, and Office Automation: BUILDING YOUR VERY OWN J.A.R.V.I.S. – ***Ed Skoudis - @edskoudis***

Pretty much every kid (and adult!) wants to have his or her very own J.A.R.V.I.S., right? Tony Stark's voice-activated smart digital assistant controls information and physical objects throughout his laboratory. But how could you make something like that secure? To that end, Ed Skoudis set out to integrate Internet of Things technologies with cloud services, voice recognition, Artificial Intelligence, and more, using a variety of off-the-shelf technologies along with some customized code to bring his lab and office to life. In this lively presentation, Ed will share his experiences in building out this technology and highlight some of the significant security concerns associated with where the Internet of Things touches the cloud and consumer-grade AI. We'll also look at with where these technologies are headed as they work their way into our every-day lives.

Metasploit Townhall – ***David Maloney - @thelightcosine, James Lee - @egyp7, Brent Cook - @busterbcook, Tod Beardsley - @todb and Lance Sanchez***

The Metasploit Open Townhall is back for its second year, exclusively at Derby Con. Come and meet some of the full time members of the Metasploit Team from Rapid7. All members of the community are encouraged to come, ask questions and give feedback. Some things we're particularly interested in hearing from you, our community, include What parts of Metasploit do you find most useful? What problems do you run into in Metasploit that cause you a lot of pain or trouble? What things is Metasploit not doing currently, that you'd like for it to start doing? Or maybe you have some questions about open source security in general, that's cool too. Whatever is on your mind, come and talk with us.

Data Obfuscation: How to hide data and payloads to make them "not exist" (in a mathematically optimal way) – ***Parker Schmitt - @parkerschmitt***

Many times the answer to any question about cryptography is: "never roll your own crypto". While the logic behind this is understandable it has become a bit of a lost art. Despite the fact that for the most part standard crypto used in normal situations works; when trying to hide the existence of encrypted data alltogether it is far from an optimal solution.

Most modern crypto is designed with the fact that the evesdropper knows that an encrypted message exists. However these days with ssl proxys, reversing antivirus, and "anti-crypto" law proposals the assumption that having an evesdropper knowing the existence of said crypto is no longer an easy concession. Despite the fact of many "next-gen" antiviruses failing to detect many obfuscation methods using algorithms such as AES for encrypting a payload is the WRONG way. The reason they are not detected is such an antivirus is just not looking for traces of such an algorithm. From a forensics standpoint, if you're using AES the private key is on the victim's machine for example. In addition, the permutations or S-Boxes are well known permutations and easy to spot in your algorithm.

This talk will be on how to design algorithms to make the existence of the cryptography unknown. We will keep some of it high level but also show how to properly implement your own cryptography and/or steganography in such a way that the evesdropper doesn't know it exists. We will talk about side channels and how to keep out of band and/or homemade crypto "cryptographically strong" but also how to generate it on the fly so that no only can you encrypt data in side channels, you can generate a new algorithm on the fly. We want to make it so the randomness of the algorithm itself is "cryptographically strong" Even though many next-gen antivirus fails at such detection as it inproves we need to study obfuscation as much as the mathematics and/or science of standard cryptography.

1:00pm–1:50pm

Writing malware while the blue team is staring at you – *Mubix "Rob" Fuller - @mubix*

Malware authors and reverse engineers have been playing cat and mouse for a number of years now when it comes to writing and reversing of malware. From nation state level malware to the mass malware that infects out of date grandmas and grandpas the different types of malware employ a myriad of techniques to stop those who look at it from guessing the true intent. This talk will be about some of the unorthodox methods employed by some malware to stay hidden from, or out right ignore the reverse engineering community.

Mind Reading for Fun and Profit using DISC – *Christopher Hadnagy - @humanhacker*

Learning to profile a target is a key element to social engineering. Learn how to use a quick and easy profiling tool to make targets feel as if you can read their minds. You will also learn how to release chemicals in your targets brains to make them more agreeable to your suggestions.

Stagefright: An Android Exploitation Case Study – *Jduck @Jduck*

Last year, Joshua disclosed multiple vulnerabilities in Android's multimedia processing library libstagefright. This disclosure went viral under the moniker "Stagefright," garnered national press, and ultimately helped spur wide-spread change throughout the mobile ecosystem. Since initial disclosure, a multitude of additional vulnerabilities have been disclosed affecting the library.

In the course of his research, Joshua developed and shared multiple exploits for the issues he disclosed with Google. In response to Joshua and others' findings, the Android Security Team made many security improvements. Some changes went effective immediately, some later, and others still are set to ship with the next version of Android—Nougat.

Joshua will discuss the culmination of knowledge gained from the body of research that made these exploits possible despite exploit mitigations present in Android. He will divulge details of how his latest exploit, a Metasploit module for CVE-2015-3864, works and explore remaining challenges that leave the Android operating system vulnerable to attack. Joshua will release the Metasploit module to the public at DerbyCon.

Top 10 2015-2016 compromise patterns observed & how to use non-traditional Internet datasets to detect & avoid them – *Arian J Evans - @arianevans and James Pleger - @jpleger*

We have seen a consistent set of patterns in attacker behaviors, and breach targets, over the last year. We often see where adversaries are repeat offenders - reusing the same recon techniques, and the same threat infrastructure (in new ways), to attack the same target again - if the target continues to play whack-a-mole treating hardening systems and investigating breaches as one-off events.

This presentation will focus on the common patterns of compromise, and adversarial behavior in the early stages of the "kill-chain", leading up to the first attack.

The goal for Red-teams & vuln-managers is to show how adversaries do recon and setup, to enable you to measure & manage your attack surface more realistically to how your adversaries will map it out. The goal for Blue-teams & IR is to show new patterns and pivots we see adversaries make, and what Internet security datasets you can use to pinpoint them.

2:00pm–2:50pm

Macs Get Sick Too – *Tyler Halfpop - @tylerhalfpop and Jacob Soo - @_jsoo_*

A brief history of Mac malware and an analysis of the current landscape will be presented to show that contrary to popular belief Macs get sick too. Methods for analysis of Mac malware as well as some anti-analysis techniques will be presented along with their application in the context of current threats to equip additional researchers with the tools to look at this often overlooked problem.

Hunting for Exploit Kits – *Joe Desimone - @dez_*

Open any security blog and you are likely to find some information on the latest Oday being exploited in the wild by one or more of the popular exploit kits. Knowing how exploit kits are evolving over time allows researchers to validate a security stack against the latest capabilities, enables red teams to repurpose the latest in-the-wild threats, and assists vulnerability researchers to stay current on the latest exploits. However, getting samples or other specific insight into these changes is hard because direct access to tools is guarded and signatures are constantly changing. How can researchers identify and collect their own samples without any static signatures? This talk will reveal an automated system that relies on behavioral exploit detection rolled into a sandbox that continually crawls popular websites for infection. The system captures a steady stream of exploit kit samples which can support a wide range of research initiatives. We will also discuss samples from popular exploit kits that have been captured with this system such as Neutrino, RIG, and Magnitude.

Rotten Potato - Privilege Escalation from Service Accounts to SYSTEM – *Stephen Breen - @breenmachine and Chris Mallz - @vvalien1*

At Shmoocon early this year, we released Potato, a new method and tool that took advantage of neglected 15 year old issues in all versions of Windows to elevate any user's privilege to SYSTEM in default configurations. We had

planned on releasing a much improved version of said tool here at Derbycon, but Microsoft had other plans. On June 14, 2016 we were surprised to find that Microsoft released MS16-075 which seems to break Potato. Luckily we still have one more trick up our sleeves that has proved useful in real-life scenarios. We will be discussing a technique based on the Potato exploit that allows for elevation from many Windows service accounts (such as those used by IIS and SQL Server) to SYSTEM in default configurations on all Windows versions.

+1,000,000 -0: Cloning a Game Using Game Hacking and Terabytes of Data – *Nick Cano - @nickcano93*

In this talk, I'll provide a window into the warchest my team used to generate over a million lines of code. In particular, we created and used game hacks to process data from tens of millions of hours of in-game data and use the results to generate copies of a game's map, monsters, quests, items, spells, non-playable characters, and more. We also used a wiki crawler to obtain a large amount of data, generate additional code, and guide our cheat scripts in what to look for, clarify, and ignore.

After explaining our end-game vision, I'll dive deep into the architecture of the game client, server and protocol. Once that's out of the way, I'll talk about the different types of hacks we used, how they work, and what data they were able to obtain. Once that's out of the way, I'll round out the story by explaining exactly what type of data we gathered and what parts of our toolkit we used to gather it.

This project isn't exactly applicable a typical day-in-the-life of a security professional, but it is a cool and informative look into the fun side of security. It shows how the same deeply technical techniques that are used to pentest, man-in-the-middle, and create malware can be used for more whimsical projects. My hope is that this talk not only provides some unbelievable anecdotes, but also arms the audience with an improved ability to creatively apply their hacking skills to similar tasks.

3:00pm–3:50pm

A Year in the Empire – *Will Schroeder - @harmj0y and Matt Nelson - @enigma0x3*

PowerShell is an ideal platform for building a new class of offensive toolsets and parties on both sides of the red and blue divide have begun to take notice. Driving some of this newfound awareness is the Empire project - a pure PowerShell post-exploitation agent that packages together the wealth of new and existing offensive PowerShell tech into a single weaponized framework. Since its release a year ago, the Empire project has garnered dozens of additional modules from the offensive community in addition to signatures and mitigations on the defensive side. This presentation will take you through the design considerations for Empire, the community contributions, its enhanced capabilities, its redesigned C2 system, and the new RESTful API. Welcome to the Empire.

Next Gen Web Pen Testing: Handling modern applications in a penetration test – *Kevin Johnson - @secureideas and Jason Gillam - @JasonGillam*

As technology advances and applications make use of newer technology, our penetration testing techniques and methods have to keep up. In this presentation, Jason Gillam and Kevin Johnson of Secure Ideas will walk attendees through new web technologies and how testing methods can change to handle the nuances. Some examples of technologies and changes that will be discussed during the talk are; HTTP/2, CSP, CORS and RESTful APIs. During the presentation, Kevin and Jason will walk through each new system or feature and methods to test it. After presenting these techniques, Jason and Kevin will walk through the new modern vulnerable application and the release of the new SamuraiWTF 4.0.

DevOops Redux – *Ken Johnson - @cktricky and Chris Gates - @carnal0wnage*

In a follow-up to the duo's offensive focused talk "DevOops, How I hacked you", they discuss defensive countermeasures and real experiences in preventing attacks that target flaws in your DevOps environments. In this talk, Chris and Ken describe common ways in which DevOps environments fall prey to malicious actors with a focus on preventative steps. The team will present their recommended approach to hardening for teams using AWS, Continuous Integration, GitHub, and common DevOps tools and processes.

To Catch a Penetration Tester: Top SIEM Use Cases – *Ryan Voloch and Peter Giannoutsos*

Every blue team should have a Chris Hansen for catching penetration testers! We surveyed multiple penetration testers and security professionals to collect the best and most useful SIEM detection use cases. The goal of the use cases is to detect a penetration tester/external attacker in a typical enterprise environment. The top use cases will be reviewed. This talk is designed to help blue teams mature their detection and SIEM programs.

4:00pm–4:50pm

PowerShell Secrets and Tactics – *Ben0xA - @ben0xa*

It used to be that most people were just starting to hear about PowerShell. Over the last 3 years, this has changed dramatically. We now see Offensive and Defensive PowerShell tools, exploits specifically leveraging PowerShell and WMI, and more organizations are starting to be intentional for detection and monitoring of PowerShell scripts and commands. With this visibility, it is becoming a game of cat and mouse to leverage and detect PowerShell. In this talk, I will highlight some secrets I use to ensure my PowerShell exploits are successful and some unique tactics which will bypass common defensive controls. I will also walk you through the creation of a custom PowerShell C# DLL which you can use to compromise your target. If you want to code with me, be sure to bring a laptop with Visual Studio 2013 or later installed.

Beyond The 'Cript: Practical iOS Reverse Engineering – *Michael Allen - @_dark_knight_*

There is an app for everything these days. And if you are current on your Infosec news you know every new app comes with its own vulnerabilities. One class of bugs has been relatively easy to find, with frameworks becoming increasingly available to help.

But more and more developers are hardening their apps against common issues using jailbreak detection and best practices, and some of the easy issues are starting to dry up.

Luckily for the top testers, there is another class of bug that can still (and only) be found with deeper knowledge of iOS and its underlying assembly code.

The aim of this talk is to build a bridge between the mundane methodologies and vulnerabilities that everyone can find (and that are now being defended against), and a new approach that finds additional bugs that require assembly knowledge to discover.

The talk looks at the fundamentals of reversing, a primer on iOS architecture, binary patching, reversing MACH-O binaries, and ends with some real-world examples involving jailbreak detection.

Attendees will leave with a better understanding of the reversing process as it applies to iOS, and each attendee will leave with a basic assembly-based iOS testing methodology.

.... and bad mistakes I've made a few..... – *Jayson E. Street - @jaysonstreet*

In an industry that does so much to uncover and expose the mistakes of others. Which don't get me wrong is a valuable service in helping to increase security by the discovery of these vulnerabilities. It seems everyone though is very shy about pointing out their own failures! I've decided that I could help teach others valuable lessons I learned by showcasing three failures I've had in Blue Team. Three failures I've had in Red Team and three failures I've had in this community. I once read that a smart person learns from their mistakes. A wise person learns from the mistakes of others! So please take a moment to listen to me trying to help you become a little bit wiser! :)

No Easy Breach: Challenges and Lessons from an Epic Investigation – *Matthew Dunwoody - @matthewdunwoody and Nick Carr - @itsreallynick*

Every IR presents unique challenges. But — when an attacker uses PowerShell, WMI, Kerberos attacks, novel persistence mechanisms, seemingly unlimited C2 infrastructure and half-a-dozen rapidly-evolving malware families across a 100k node network to compromise the environment at a rate of 10 systems per day — the cumulative challenges can become overwhelming.

This talk will showcase the obstacles overcome during one of the largest and most advanced breaches Mandiant has ever responded to, the novel investigative techniques employed, and the lessons learned that allowed us to help remediate it.

5:00pm–5:50pm

CrackMapExec - Owning Active Directory by using Active Directory – *Marcello Salvati - @byt3bl33d3r*

Over the past few years there have been incredible research and advances in offensive Active Directory techniques: we are now able to essentially use Active Directory against itself by abusing builtin Microsoft features (e.g. 'Living off the Land').

The introduction of PowerShell has only made this easier by allowing access to low-level API calls through a powerful scripting language: reflectively executing code in memory, finding actively logged in domain administrators and much more is now all possible using only built-in Windows features.

The techniques have advanced very quickly, and now as pentesters we need a tool that can take full advantage of these techniques.

Look no further than CrackMapExec! Awkwardly named, fully open-source and hosted on Github: it aims to be a one-stop-shop for all of your offensive Active Directory needs by combining the power of Python, Powersploit (https://github.com/PowerShellMafia/PowerSploit) and the Impacket library (https://github.com/CoreSecurity/impacket)!

Taking inspiration from previous tools such as:

- smbexec (https://github.com/pentestgeek/smbexec)
- smbmap (https://github.com/ShawnDEvans/smbmap)
- credcrack (https://github.com/gojhonny/CredCrack)

It allows you to quickly and efficiently import credentials from Empire and Metasploit, replay credentials, pass-the-hash, execute commands, powershell payloads, spider SMB shares, query LDAP, dump SAM hashes, the NTDS.dit, interact with MSSQL databases and lots more in a fully concurrent pure Python script that requires no external tools and is completely OpSec safe! (no binaries are uploaded to disk!).

We will be taking a fairly deep dive into CrackMapExec's internals to explain how it works under the hood, outlining the key differences and improvements between it and it's predecessors (using primarily live demos) while also explaining in detail how the attacks actually work from a network and domain standpoint and how to properly defend against them.

Adaptation of the Security Sub-Culture – *Rockie Brockway - @RockieBrockway and Adam Hogan - @adamwhogan*

Infosec is a lot like punk rock. We're an odd sub-culture full of odd people driven by oddly intense passion.

In response to increasingly sophisticated attacks, and a series of well televised breaches, the infosec industry has been calling for organizations to "change the security culture." But like other sub-cultures we have issues communicating our ideas to the masses. We have a duty to evangelize for security in a way that doesn't expect infosec militants but rather naturally grows a security culture from the bottom up.

You can't teach someone to like punk rock. But over time the Sex Pistols' influence eventually led to Offspring, Green Day and Blink-182, and fans of those successful bands were not typically part of the die-hard punk rock sub-culture. Our culture can, and will, adapt this way. If we want to scale we also need to go pop - but we can't do it overnight.

We will give an introduction to complexity theory and the psychology of belonging to a sub-culture. We will show how you can grow your security team and broaden awareness with these ideas in mind - and organizational change is sure to fail.

Better Network Defense Through Threat Injection and Hunting – *Zach Grace - @ztgrace and Brian Genz - @briangenz*

Traditional penetration testing and red team engagements typically focus on identifying single attack paths and how organizations can fix vulnerabilities to shut those paths down. The results of these engagements are a reduced risk from eliminating a single attack path, but rarely lead to an improved defensive skill set.

This talk will introduce the Threat Detection Maturity Model, a security detection and testing framework to more closely integrate red and blue team operations with the goal of measurably improving defensive capabilities. The framework is designed to measure the effectiveness of the blue team's defensive capabilities using a capability maturity model across the attack lifecycle. We'll demonstrate how "threats" are injected into an environment to enable a hunt team or SOC to improve their skill sets and validate the effectiveness of their security tooling.

Hacking Lync (or, 'The Weakest Lync') – *nyxgeek - @nyxgeek*

Thinking of exposing Lync externally? Think twice before painting a big bullseye on your organization.

6:00pm–6:50pm

Exploiting First Hop Protocols to Own the Network – *Paul Coggin - @PaulCoggin*

This talk will focus on how to exploit a network by targeting the various first hop protocols. Attack vectors for crafting custom packets as well a few of the available tools for layer 2 network protocols exploitation will be covered. Defensive mitigations and recommendations for adding secure visualization and instrumentation for layer 2 will be provided.

Outlook and Exchange for the Bad Guys – *Nick Landers - @monoxgas*

External mail via Exchange is one of the most common services offered by organizations today. The Microsoft Office suite is even more prevalent making Outlook the most common mail client around. This talk focuses on the abuse of these two products for the purpose of gaining code execution inside remote networks. Subjects include E-Mail and password scraping, OWA/EWS brute forcing techniques, and new research into abusing Outlook mail rules for remote code execution. Learn about the capabilities of client side rules, the underlying Windows APIs, and how to modify these rule objects to make phishing attacks obsolete.

It's Never So Bad That It Can't Get Worse – *Valerie Thomas - @hacktress09 and Harry Regan - @geezbox*

Disaster recovery, emergency response and business continuity plans are usually developed when no disaster exists. We think we've covered all contingencies. We think we've trained all the appropriate players. We've tested. We've re-tested. We think we're ready to face whatever event there is looming out their with our name on it! The real world has a nasty habit of triggering disasters at the least opportune time, often featuring a twist that throws plans into disarray.

This presentation focuses on three reasonable, real-world BCP plans, each of which had a fatal flaw. We will discuss elements that should be in a plan beyond the normal guidance from the Disaster Recovery Institute (DRI) and a set of actions that should be included in planning and preparation.

AWShit. Pay-as-you-go Mobile Penetration Testing – *Nathan Clark - @Infanamecheap*

Tired of trying to carry every device to an engagement? Learn how to make mobile device a pentesters dream. All open source and free!

7:00pm–7:50pm

From Commodity to Advanced (APT) malware, are automated malware analysis sandboxes as useful as your own basic manual analysis? – *Michael Gough - @HackerHurricane*

According to Mandiant M-Trends, their customers average Mean Time to Discovery (MTTD) for breaches in 2012 was 416 days, 2014 was 205 days and 2015 was 146 days. In 2015 for those Mandiant customers that detected a breach themselves was 56 days! Unfortunately, the average days for a third party to report your company has been breached is 320 days. As an industry we still need to vastly improve since companies get compromised within an hour and the entire organization within a day and valuable data begins to leak shortly thereafter. We CAN do better!

So how do we reduce our detection time? How can we save serious $$$ by either not using an IR firm and doing it ourselves or saving $$$ by reducing how long the IR firm is on site? Many of us cannot afford an IR firm at a DROP of a TABLE. The ultimate goal and challenge to all of us is to learn how to discover a compromise ourselves and avoid a breach. We as an industry must get better at discovery, detection and response and do it faster, much faster. This talk will share how, where to begin and a new tool for Windows to help us do it ourselves. Learn from those of us that have been through it because the criminals can own you in a day and it is still taking a year to receive the OH SH*T call.

Defeating The Latest Advances in Script Obfuscation – *Mark Mager - @magerbomb*

In this age of increasingly sophisticated and devastating malware, adversaries still rely on a multitude of scripting languages and frameworks (e.g. JavaScript, VBA, PowerShell, VBScript) as key components of an attack scenario. These scripts tend to employ obfuscation techniques in order to obscure their true intent and avoid detection by endpoint protection products. Though significant

advances have been made in recent years in packing and obfuscating compiled binaries, script obfuscation can still be defeated with time and a determined analyst. This talk will cover some of the most recently seen advanced obfuscation techniques employed by APTs, exploit kits, and other malware authors along with proven methods for circumventing and decoding these techniques. I will then apply these methods to guide the audience through the deobfuscation of a fully obfuscated script. Audience members will walk away with a solid understanding of how common obfuscation techniques are employed in scripting languages along with how they can be defeated.

SATURDAY – 9.24.

9:00am–9:50am

Breaking Credit Card Tokenization Without Cryptanalysisk – *Tim MalcomVetter - @malcomvetter*

Credit Card Tokenization is a very popular antidote to costly and time-consuming PCI regulations, but are all implementations equally secure? Early studies on tokenization focused on the cryptanalysis of the token generation process, especially when early implementations sought to create 16 digit numeric tokens to satisfy constraints in legacy commerce systems. Fast forward to 2016, most of those problems do not exist today; however, anecdotes from consulting with Fortune 500s suggest other insecure properties not involving crypto can vary and emerge in tokenization systems.

This talk will dig into several sanitized examples from consulting engagements which reduce "PCI Compliant" Credit Card Tokenization from "silver bullet" to "speed bump" status when big-picture security controls are missing. Specifically: abusing separation of duties by rogue partial insiders via public APIs commonly found in e-commerce applications; discovery of accidental side channels of critical information flow, such as timing analysis or response differentiation, which can be abused to reveal full PANs (primary account numbers); whether DevOps cultures could promote rogue admins abusing tokenization presentation logic implemented in JavaScript; and for good measure: some common programming defects which at best render tokenization pointless, and at worst could allow for a breach. With each example, we'll look at potential solutions.

Deploying PAWs as Part of a Strategy to Limit Credential Theft and Lateral Movement – *Bill V - @blueteamer*

Bruce Schneier sums up credential theft much better than I can. He said the following in a blog post earlier this year:

The most common way hackers of all stripes, from criminals to hacktivists to foreign governments, break into networks is by stealing and using a valid credential. Rob Joyce, the head of the NSA's Tailored Access Operations (TAO) group -- basically the country's chief hacker -- gave a rare public talk at a conference in January. In essence, he said that zero-day vulnerabilities are overrated, and credential stealing is how he gets into networks. Stealing a valid credential and using it to access a network is easier, less risky, and ultimately more productive than using an existing vulnerability, even a zero-day.

Privileged Access Workstations (PAWs) are hardened admin workstations implemented to protect privileged accounts. In this talk I will discuss my lessons learned while deploying PAWs in the real world as well as other techniques I've used to limit exposure to credential theft and lateral movement. I hope to show fellow blue teamers these types of controls are feasible to implement, even in small environments.

Business Developement: The best non-four letter dirty word in infosec. – *Scott Lyons - @Csp3r_th3_ghOst and Joshua Marpet - @Quadling*

Everyone today wants to start their own business. I mean Dave Kennedy did it, how hard could it be???? (Love you, Dave!) So you gather your team and you can do the pen-testing, and Jimmy over there can handle Incident Response, right? So what's the big deal? Why aren't customers knocking down my door???? Don't they know how awesome we are!?!?!??!1?11!?

Business Development. No, it's not a dirty word. BUSINESS DEVELOPMENT is how you make money. It's how you put food on the table and a roof over your head. You can do the work. Cool! Where's the work coming from? You know, those things called…. customers?

Let's address the mysteries of business development. We will take you from the initial meeting in the boardroom, through identification of stakeholders, getting the Statement of Work hammered out and signed, finding the ideal employee, and getting the job done all while effortlessly making the money. We will also cover what happens when you screw up each and every single step of the process, as well. (Trust us, you will! We did!) :)

We'll discuss the differences between a product based business and a service based business, explain the process, the funnel, the problems, the success stories. And it's all real.

Bottom line: Starting a business is easy! Keeping the doors open? Not so much.

"If it was easy, everyone would do it!" - Albert Einstein, or maybe Abraham Lincoln

Tool Drop 2.0 - Free As In Pizzak – *Scot Berner - @slobtresix and Jason Lang - @curiOusJack*

Who doesn't love free tools? We certainly do, and as pentesters, we use them all the time. Now we get to give back to the community we love! We're releasing tools we've written over the past year (again). Wireless attacks, macro attacks, AWS pentesting automation, hacking Exchange web services, as much as we can fit in the time we have!

This talk will focus mostly on red team tools. Blue team, you are absolutely encouraged to come so you can see what you're up against. We will include defensive measures wherever applicable.

If you love free stuff, good stories, and are sick of the slides (this talk will be all demo), you'd better be here. Derbycon exclusive!

10:00am–10:50am

Attacking EvilCorp: Anatomy of a Corporate Hack – *Sean Metcalf - @PyroTek3 and Will Schroeder - @harmj0y*

With the millions of dollars invested in defensive solutions, how are attackers still effective? Why do defensive techniques seem to rarely stop or slow down even mid-tier adversaries? And is there anything the underfunded admin can do to stop the carnage?

Join us in a shift to "assume breach" and see how an attacker can easily move from a single machine compromise to a complete domain take over. Instead of "death by PowerPoint," see first-hand how a fictional corporation suffers "death by a thousand cuts."

The fictional EvilCorp presents their top defensive tools and practically dares someone to attack the network. The battle of Red vs. Blue unfolds showing EvilCorp's network submit to the unrelenting attacks by an experienced adversary. When the dust settles, the Red Team looks victorious. But what, if anything, could have tipped the scales in the other direction?

In this demo-heavy session (several demos are shown to demonstrate modern attack effectiveness), we showcase the latest attack techniques and ineffective defenses still used to protect companies. Defense evasion tools and techniques are detailed as well as attack detection methods. Effective mitigation strategies are highlighted and the Blue Team is provided a roadmap to properly shore up defenses that can stop all but the most determined attacker.

Living Off the Land 2: A Minimalist's Guide to Windows Defense – *Matt Graeber - @mattifestation*

The "living off the land" philosophy, as applied to InfoSec, is the idea that one can thrive using mostly the tools present in a target environment in an effort to remain hidden from an adversary. While historically this philosophy has been applied to offense, it is equally applicable to defense. A capable defender, ideally, should introduce a minimal forensic footprint into an environment suspected to be compromised. Additionally, informed defenders should have an awareness of attacker objectives which includes performing reconnaissance against common security products, most of which consume a substantial OS fingerprint. This talk aims to introduce defenders to defensive capabilities built-in to all versions of Windows which are likely to leave adversaries in dark as to what defensive mechanisms are in place. Expensive defensive products are not always the solution when you're already sitting on a goldmine of free, unexploited capabilities.

Point of Sale Voyuer- Threat Actor Attribution Through POS Honeypots – *Kyle Wilhoit - @lowcalspam*

What would POS terminal cybercriminals do if they didn't know you were watching? Imagine you could understand and see a clear connection between a payment terminal compromise, credit card numbers getting stolen from those terminals, and ultimately their sale on the underground. Attribution of attackers is often difficult, especially when dealing with point of sale terminal breeches. Trying to establish tools, tactics and procedures in order to better understand the adversary also takes time, effort, and dedicated resources. Using a combination of physical and virtual honeypots, we tracked POS attackers from the initial infection all the way to the sale of fake credit cards on underground forums. In this new research, we cover the malware, TTP's, and attack chain behind several POS actors against our honeypots. Finally, learn about a tool we created and used that aided in the analysis of attacks, file drops, and communications– FileGrabber – that we are going to release at the end the talk.

The Art of War, Attacking the Organization and Raising the Defense – *Jeremy Mio - @cyborg00101, David Lauer - @securid and Mike Woolard - @Woolyб Bear*

The most effective way into an organization, cute cat pictures and free tickets to DerbyCon… the easiest and quickest way into an organization, attacking the weakest link, humans. There are many campaigns in the wild conveying "Cyber Security" being a shared responsibility across the organization, but how can we expect that when we do not prepare our fellow employees? We need to properly prepare our employees, managers, technical folk, and even the Executives for the security battle ground. Militaries do not train their generals, sergeants, and ground soldiers with the same material and techniques, and neither should we for security awareness training. Join us and an old friend, Sun Tzu, to prepare the war and battles we are facing from all sides of our organization.

12:00pm–12:50pm

Phishing without Failure and Frustration – *Jay Beale - @jaybeale*

Your first time phishing professionally could be full of frustration and failure. Picture it:

You want to phish your company or your client. You've never done this for work before, you've got a week to do it, and you figure that's plenty of time. Then someone objects to the pretext at the last minute. Or spam filters block everything. Or you decide to send slowly, to avoid detection, but the third recipient alerts the entire company. Or you can only find 5 target addresses. We've all been there on our first professional phishing exercise. What should be as easy as building a two page web site and writing a clever e-mail turns into a massively frustrating exercise with a centi-scaled corpus of captured credentials.

In this talk, we'll tell you how to win at phishing, from start to finish, particularly in hacking Layer 8, the "Politics" layer of the OSI stack that's part of any professional phishing engagement. We'll share stories of many of our experiences, which recently included an investigation opened with the US Security and Exchange Commission (SEC). Finally, we'll tell you how we stopped feeling frustrated, learned to handle the politics, and produced successful phishing campaigns that hardened organizations at the human layer, and started to screw things up for the bad actors.

I don't give one IoTA: Introducing the Internet of Things Attack Methodology.– *Larry Pesce - @haxorthematrix*

Anti-Forensics AF –*int0x80 (of Dual Core) - @dualcoremusic*

This presentation is the screaming goat anti-forensics version of those "Stupid Pet Tricks" segments on late night US talk shows. Nothing ground-breaking here, but we'll cover new (possibly) and trolly (definitely) techniques that forensic investigators haven't considered or encountered. Intended targets cover a variety of OS platforms.

Managed to Mangled: Exploitation of Enterprise Network Management Systems – *Deral Heiland - @Percent_x and Matthew Kienow - @HacksForProfit*

Network Management Systems (NMSs) are widely deployed in medium and large organizations to map and control network and host infrastructure, and provide an excellent attack surface. NMSs are information rich for an attacker, saving reconnaissance time and providing a pivot point to hide their network activity in the background noise. The talk explores many NMS attack vectors, including persistent cross-site scripting (XSS), format string vulnerabilities, command injection, SQL injection and forced browsing to take control of the NMS and authenticated user's host. Using live demonstrations we explore attack delivery, execution and factors that control the success of each attack. In conclusion, we discuss overall risk factors and mitigation techniques for providing protection against these attacks.

1:00pm–1:50pm

New Shiny in Metasploit Framework – *egypt - @egyp7*

This Derbycon tradition will . I'll cover some of the awesome new capabilities added to the Framework in the last 12 months, including improvements to meterpreter, post exploitation, and more. `git log --since="2015-09-23"`

Five year checkup: the state of insulin pump security – *Jay Radcliffe - @jradcliffe02*

Five years ago, my security research on insulin pump hacking exposed a chilling lack of security within a device type that, by design, maintains health. It is now time to see what has actually changed for the better, what has stayed the same, and what has gotten worse regarding the security of modern insulin pumps. Has the industry made progress? Have the medical standards of care improved in any way? Are we, as patients, now better protected against the real and proven security threat?

At the same time, we must also consider the newer trend of people who are using medical technology to develop "side projects" such as the DIY artificial pancreas project. These initiatives are not subject to oversight from any legal body, are not required to make any security considerations, or are not developed in cooperation with any medical providers. Do they introduce new risks for patients and healthcare organizations alike?

The focus of this presentation is on new, original research into the design flaws of insulin pump technology. We will provide insight into the path we still have ahead of us with regards to security in the medical industry. Our presentation will cover multiple new vulnerabilities, which can be exploited from a distance. The impact of our vulnerabilities can be fatal, and with the pervasiveness of such technology become more and more likely to be exploited by attackers.

We will include the perspective of rapidly changing risk, useable defensive techniques, and the progress in each of these areas into the narrative of our talk.

Finally, our talk will also cover a review of the milestones of medical security, both in advancement and setbacks, over the last five years.

Penetration Testing Trends – *John Strand - @strandjs*

We all know and love the yearly reports from Verizon and Mandiant. They break down the various Incident Response gigs they worked on during the previous year. But what about the other side of the coin? What about penetration testing companies? What are they seeing? In this presentation, John will share a breakdown of the penetration tests BHIS performed over the last year. He will discuss how most organizations are improving - and where they are still failing. More importantly, he will share a frightening trend – a trend that could have earth-shattering repercussions for the entire security industry. Dum, dum, DUMMMMMMM!!!

Garbage in, garbage out: generating useful log data in complex environments – *Ellen Hartstack and Matthew Sullivan*

Log messages. Your company probably has billions of them; but are they useful, or just noise?

Having meaningful log data is a critical part of running a successful IT shop or hosted web application. How often does your user hit that weird edge-case bug? How many times has this IP address accessed our web front-end using a non-standard browser? How much processing time could we save our customer by refactoring that one function? In many environments, finding answers to these types of questions can be difficult or even impossible. Sure, the data might be there, but is it even useful?

In this sysadmin and developer-focused talk, we'll discuss ways to provide more meaningful and parsable log data, whether using an off-the-shelf product, open source, or written in-house. We'll also briefly demonstrate how tools like Splunk or ELK stack can be leveraged to make better decisions, saving time and money.

2:00pm–2:50pm

Embrace the Bogeyman: Tactical Fear Mongering for Those Who Penetrate – *FuzzyNop - @FuzzyNop*

When it comes to cyber penetration, evolving threat landscapes mandate advanced persistent tac…. ha ha, just kidding. Look, let's be real, as an internal red team things can get really weird. A day job carrying out a company's most apocalyptic self-destructive fantasies presents a strange

duality of helping and hurting. General public and corporate fear of 'hackers' has been both a blessing and a curse. You might say it's a gray area, but is it really that simple? In this talk i'll share the ups, downs, and lessons learned during my adventures as the corporate bogeyman.

Introducing DeepBlueCLI, a PowerShell module for hunt teaming via Windows event logs – *Eric Conrad - @eric_conrad*

A number of events are triggered in Windows environments during virtually every successful breach, these include: service creation events and errors, user creation events, extremely long command lines, compressed and base64 encoded PowerShell functions, and more.

Microsoft has added a wealth of blue team tools to its operating systems, including native support of logging the full command line used to launch all processes, without requiring 3rd party tools (or Sysmon). KB3004375 adds this feature to Windows 7 and Server 2008R2.

DeepBlueCLI can automatically determine events that are typically triggered during a majority of successful breaches, including use of malicious command lines including PowerShell.

Using Binary Ninja for Modern Malware Analysis – *Dr. Jared DeMott - @jareddemott and Mr. Josh Stroschein - @jstrosch*

After a quick intro and outline we jump into an exciting talk about how to do advanced malware analysis on modern samples. On top of that, we introduce a new reverse engineering tool: Binary Ninja. Typically, IDA pro rules the roost.

But IDA is too expensive for most mortals. It's time for a new tool to take the spot light. We describe a hot, new malware - and discuss how well BN did compared to IDA for analysis. We conclude with advice for further BN development.

Fuzzing basics…how to break software – *grid (aka Scott M)*

Ever wanted to break software? You know you want to…it's fun! In this talk, I will share some tools & techniques I've used to improve software by breaking it.

3:00pm–3:50pm

How to Social Engineer your way into your dream job! – *Jason Blanchard - @BanjoCrashland*

Does anyone read these descriptions? Yeah… you? That's awesome! Want to come to an incredible talk given by a professional social engineer? No… oh, ok… Wait! Come back! Alright, this talk is about how you can use the skills, concepts, and tools of social engineers and marketers to put yourself into the right place, with the right skills, for the job you've always wanted. After 40 minutes of this talk, you'll either hate Jason Blanchard because he's given you so many possible ways to get "unstuck" or you'll… nah, you'll probably just hate him. This talk will be unforgettable (and hilarious). #chickenwing

Attackers Hunt Sysadmins - It's time to fight back – *Lee Holmes - @Lee_Holmes*

What do the NSA, APT groups, and run-of-the-mill attackers have in common? They. Hunt. Sysadmins. After all, what's a better way to compromise an entire infrastructure than to target the folks with complete and unconstrained access to it?

It's time to fight back.

In this talk, we introduce PowerShell Just Enough Administration, a powerful platform capability that lets you add role-based access controls to your existing PowerShell-based remote management infrastructure.

Scripting Myself Out of a Job - Automating the Penetration Test with APT2 – *Adam Compton - @tatanus and Austin Lane - @capndan*

Nearly every penetration test begins the same way; run a NMAP scan, review the results, choose interesting services to enumerate and attack, and perform post-exploitation activities. What was once a fairly time consuming manual process, is now automated!

Automated Penetration Testing Toolkit (APT2) is an extendable modular framework designed to automate common tasks performed during penetration testing. APT2 can chain data gathered from different modules together to build dynamic attack paths. Starting with a NMAP scan of the target environment, discovered ports and services become triggers for the various modules which in turn can fire additional triggers. Have FTP, Telnet, or SSH? APT2 will attempt common authentication. Have SMB? APT2 determines what OS and looks for shares and other information. Modules include everything from enumeration, scanning, brute forcing, and even integration with Metasploit. Come check out how APT2 will save you time on every engagement.

Hacking for Homeschoolers: STEM projects for under $20 – *Branden Miller - @f0zziehakz*

Lets face it, homeschoolers have a limited budget. This talk will show you how to teach STEM at home with minimal amount of money. Each project has been built in my home by my kids (ages 9+). You only have the interwebz, tin foil, and foam board? HDTV antenna! You have a couple of empty 2 Liter bottles, PVC pipe, bicycle pump, and duck tape? Soda bottle rockets! MacGyver will be jealous! Your kids will love it! Bring them too!

4:00pm–4:50pm

Medical Devices: Pwnage and Honeypots Make STEHM Great Again – *David Schwartzberg - @DSchwartzberg and Chris Sistrunk - @chrissistrunk*

Internet security threats continue to rise. Comparatively to the growing threats, there are too few security professionals in the field who are qualified to respond effectively. This session explores STEM's success but the importance to include 'Hacking' into the acronym as a means to introduce a wider audience of future potential security practitioners to address the workforce shortage. A combination of use cases, hacking success stories, and lessons learned, we discuss the benefits of introducing younger students to ethical hacking

and information security. We will future explore various programs which introduce basic skills through to advanced techniques used in the penetration testing field. Given the future of Internet security's reliance upon a fresh crop of graduating students, the session will describe how breaking the mold of traditional education systems are already embracing STEHM without understanding how to define rubrics. STEM is good, but it's time to Make STEHM Great Again.

Python 3: It's Time – *Charles L. Yost - @charleslyost*

Are you being indecisive? Are you still using Python 2 for your personal or professional projects? If so, I've got good news, it's time to move to Python 3. Have you wanted to start developing in Python, but could not decide which version to start with? There has never been a better time than now to start using Python 3. We will go over the advantages Python 3 offers, and the reasons it is a good choice for any new projects. We will also review ways to make Python 2 code compatible with Python 3. Finally we will talk about how to get started in Python 3 while maintaining environments allowing you to continue working with your Python 2 code until you can port it to Python 3.

DNS in Enterprise IR: Collection, Analysis and Response – *Philip Martin - @SecurityGuyPhil*

DNS is an often-overlooked and under-tooled area of security data collection, analysis and response. We will first review existing tools and deployment choices for collecting DNS data and release the 1.0 version of my own network DNS capture tool, gopassivedns. We will then explore several example analytical approaches to large scale DNS data, including approaches to finding DNS tunneling and discovering attacker infrastructure. Finally, we take a look at how DNS can play a part in remediation and release a second tool, a RESTful interface to RPZ, goRPZ. Attendees will walk away able to implement or improve DNS collection and analysis in their environments.

Need More Sleep? REST Could Help – *Drew Branch*

Increasingly, RESTful APIs are utilized to provide a communication avenue for web servers and clients to exchange data via HTTP(S). Historically SOAP APIs were used for this purpose however, implementation, client development, and documentation have been proved more complicated than that of REST. Further, REST provides a greater level of performance and scalability over SOAP, which adds to the benefits of using RESTful APIs.

In this talk, key differences between SOAP and REST and core REST concepts will be discussed as well as testing methodologies and techniques that an analyst or developer could utilize to discover vulnerabilities within implementations of RESTful APIs. Burp Suite will be used to demonstrate testing when discussing focus areas of interests of a RESTful API, which will include authorization and input validation.

Attendees should leave this talk with a firm understanding of RESTful APIs, how they are implemented, and how to assess RESTful APIs for vulnerabilities.

5:00pm–5:50pm

Breaking Android Apps for Fun and Profit – *Bill Sempf - @sempf*

The massive growth of internet connected smart devices like phones and toasters is truly amazing, but it also expands an attack surface for those dead-set on stealing your stuff. Making sure an Android app does what it says - and ONLY what it says - is a life skill these days. Bill will use his experience doing vulnerability analysis on Android phone apps and walk you through the process of taking an app apart. No slides, just a walkthrough from 'look here's an app in the store' to 'here's the spot in the code where it does (or doesn't) do what it says.'

So You've Inherited a Security Department, Now What… – *Amanda Berlin - @infosystir and Lee Brotherston - @synackpse*

Over the last decade, technology as a whole has exploded worldwide and corporations have struggled to keep pace. Usability and revenue creation have been the key motivating factors, ignoring the proactive design and security required for long-term stability. With the increase of breaking news hacks, record breaking data leaks, and ransomware attacks it is our job to not only scrape by with default installs but to secure our data and assets to the best of our abilities. There will always be cases where you will walk into an environment that is a metaphorical train wreck. So many of us have been there. We've walked into an environment that has exploded with technology, but no talent to manage it, no leadership to distinguish FUD from real threats, and either zero infosec budget or so much they aren't sure what to do with it. If you or someone you know are currently in this situation, we're here to help. We'll go over great steps to start with that will have little impact on budget, but a large impact on moving forward for a more secure environment. It is important to be able to implement low cost security technology and prioritize threats to show upper level management that due diligence has been done before they throw money at blinky boxes.

Reverse engineering all the malware…and why you should stop. – *Brandon Young - @bry6891*

Reverse engineering malware isn't about pulling out a bunch of IOC's anymore, hell, Cuckoo can do that just fine the majority of time. I'll admit, there are a few times when we see customized malware or a new variant that we need to RE in order to pull out some uniqueness in a quick fashion, but most static signatures can be written with a hex editor and Strings…

So why do we reverse engineer malware still? Well, who do you think builds the automated analysis tools and sandboxes? It's a group of extremely talented software developers and a few reverse engineers who are tired of spending their time writing string decoders for PlugX.

This talk will discuss some of the more menial tasks that reverse engineers are plagued with and then dive deeper into the types of projects that can really take advantage of this unique skill set along with utilizing reverse engineers to improve on your own security tools and those in our open-source community.

Remember, if Cuckoo can do it then you shouldn't have to.

Body Hacking 101 (or a Healthy Lifestyle for Security Pros) – *Nathan Magniez - @hackhunger*

Security consulting is a beast of a lifestyle. Travel, airport food, late night report writing...It leads to accumulating a spare tire and unhealthy habits. If you have wondered how to overcome this unspoken issue in our community then this talk is for you. I was there. Flying. Eating. Ignoring my health.

If you are wondering how to get started in a healthier lifestyle without the inundation of pseudo/false information from fitness magazines then this workshop is for you. Every attendee will walk away with the knowledge and ability to control their own body weight and shape their own health goals.

This will be a no non-sense, no body shaming, no bullshit approach to helping people achieve what they want out of themselves. <cliché> We all have root level privileges of ourselves...controlling that absolute power is half the battle. </cliché>

6:00pm–6:50pm

Attacking ADFS Endpoints with PowerShell – *Karl Fosaaen - @kfosaaen*

Active Directory Federation Services (ADFS) has become increasingly popular in the last few years. As a penetration tester, I'm seeing organizations opening themselves up to attacks on ADFS endpoints across the Internet. Manually completing attacks against these endpoints can be tedious. The current native Microsoft management tools are handy, but what if we weaponized them. During this talk, I will show you how to identify domains that support ADFS, confirm email addresses for users of the domain, and help you guess passwords for those users. We'll cover how you can set up your own hosted ADFS domain (on the cheap), and use it to attack other federated domains. On top of that, we'll show you how you can wrap all of the native functionality with PowerShell to automate your attacks. This talk should give penetration testers an overview on how they can start leveraging ADFS endpoints during a penetration test.

The 90's called, they want their technology back – *Stephen Hilt - @sjhilt*

Pagers are prevalent even to this day in the healthcare sectors around the world. This talk will focus on the basics of pagers, the protocols that are used, the systems that are currently using them, and the analysis of some of the pages that have been observed from researchers at Trend Micro during the project.

SUNDAY – 9.25.

10:00am–10:50am

Introducing PowerShell into your Arsenal with PS>Attack – *Jared Haight - @jaredhaight*

PS>Attack is a custom tool that was created to make it easier for Penetration Testers to incorporate PowerShell into their bag of tricks. It combines a lot of the best offensive tools from the offensive PowerShell community into a custom, encrypted console that emulates a PowerShell environment. It also includes a custom command, "Get-Attack" to act a search engine for attacks making it easy to find the right attack for any situation. In this presentation we will cover how PowerShell can be used during every part of a penetration test and how PS>Attack can help make the whole process a lot easier.

Recharging Penetration Testing to Maximize Value – *James Jardine - @jardinesoftware*

Penetration testing is one of the main standards in which organizations measure their security. We all know the drill. Spend a week or more "testing like a bad guy" and provide a report to the client indicating the findings. While this works for satisfying clients requirements defined by regulators and compliance, it produces little value for increasing their security. It is time to take another look at how penetration testing engagements can evolve with the client in mind. In this session, James will discuss how pen tests are typically consumed and ways to enhance the experience. How we can, as consultants, maximize the value of these tests.

Poetically Opaque (or other John Updike Quotes) – *hypervista - @hypervista*

This talk is an overview of the newly released security product from Intel, Software Guard Extensions (SGX), and how it can be used to harden your sensitive algorithms and data from reverse engineering by your adversaries. SGX provides hardware enforced protection of secure enclaves in the application stack that are opaque to even the most privileged processes running on the platform including the OS, hypervisors, SMM, etc. SGX takes a "zero trust" approach to its implementation and runtime operation. SGX is implemented by the inclusion of 18 new instructions to the IA-32 Instruction Set and baked into the CPU via microcode. While not perfect, SGX will help us significantly raise the anti-reverse engineering bar.

Hack Yourself: Building A Pentesting Lab – *David Boyd - @fir3d0g*

We all want to improve our skill sets, right? Reading is great, but there is no experience like actually 'doing it'. In this module, we will discuss how to build your own hacking lab from the ground up, for next to no cost. We will also discuss the various free penetration testing distributions, as well as the intentionally vulnerable virtual machines you can practice anything on from phishing, to web app testing, to exploits, and more.

11:00am–11:50am

Hardening AWS Environments and Automating Incident Response for AWS Compromises – *Andrew Krug - @andrewkrugand and Alex McCormack - @amccormack*

Incident Response procedures differ in the cloud versus when performed in traditional, on-premise, environments. The cloud offers the ability to respond to an incident by programmatically collecting evidence and quarantining

instances but with this programmatic ability comes the risk of a compromised API key. The risk of a compromised key can be mitigated but proper configuration and monitoring must be in place.

The talk discusses the paradigm of Incident Response in the cloud and introduces tools to automate the collection of forensic evidence of a compromised host. It highlights the need to properly configure an AWS environment and provides a tool to aid the configuration process.

Yara Rule QA: Can't I Write Code to do This for Me? – *Andrew Plunkett*

Yara is a powerful scanning tool that uses signatures to detect threats. It has quickly become a staple of many IT security programs. They can be used to find new samples with VirusTotal hunting, to scan endpoints, to detect malware families during sandbox or manual analysis, and for whatever other use you can come up with. New malware intelligence usually has a yara rule for detection of the malicious code, and there are many public groups that share yara rules so you need not create your own for each new threat.

Accepting public rules into your own tools and environment creates some issues, though. Will the rule run with your tool (version issues)? Is the rule written efficiently (performance issues)? Will the rule compile or have a high True Positive/ False Positive ratio (quality issues)? Do different collections of rules have overlapping signatures (duplication issues)?

This talk will discuss problems with accepting publicly available yara rules into your own tools and environment, and share code with mitigating these issues.

Java RATS: Not even your Macs are safe – *Anthony Kasza - @anthonykasza*

Java's "write once, run anywhere" features make it a popular cross-platform vector for attackers of all skill levels. This talk will perform a deep examination of historic and trending Java malware families, their capabilities and indicators, and will reveal uncommon analysis techniques to immediately help you with investigations.

The Advanced Persistent Pentester (All Your Networks Are Belong 2 Us) – *Beau Bullock - @dafthack, Derek Banks - @0xderuke and Joff Thyer - @joff_thyer*

An Advanced Persistent Pentester is always willing to go the extra mile, working smarter, and harder to achieve success. An Advanced Persistent Pentester is always willing to go off script, creatively inventing new concepts, new tools, and techniques to get the job done. We all use automated tools and techniques to construct advanced malware which allows for expeditious entry, escalation, persistence and post exploitation during engagements. What happens when the standard tools, and techniques are just not good enough?

This talk will examine several different escalation, lateral movement, and post exploitation case studies talking about the various creative approaches in solving problems along the way, capturing the flag(s), and pushing to the extremes of threat modeling the real world information security environment. It was reported that in 2015 it took an average of 146 days to detect an attacker. How can successfully mimic the impact of having that much time to pillage a network in less than a week?

12:00pm–12:50pm

Invoke-Obfuscation: PowerShell obFUsk8tion Techniques & How To (Try To) D""e`Tec`T 'Th'+'em' – *Daniel Bohannon - @danielhbohannon*

The very best attackers hide their commands from A/V and application whitelisting technologies using encoded commands and memory-only payloads to evade detection. These techniques thwart Blue Teams from determining what was executed on a target system. However, network defenders are catching on, and state-of-the-art detection tools now monitor the command line arguments for powershell.exe either in real-time or from event logs.

We need new avenues to remain stealthy in a target environment. So, this talk will highlight a dozen never-before-seen techniques for obfuscating PowerShell command line arguments. As an incident responder at Mandiant, I have seen attackers use a handful of these methods to evade basic command line detection mechanisms. I will share these techniques already being used in the wild so you can understand the value each technique provides the attacker.

Next, I will introduce three new layers of obfuscation that can be applied to any PowerShell command. You can use each layer independently, or stack them together to prevent any one technique becoming an easy signature for defenders. The first layer directly manipulates PowerShell and .Net cmdlets, functions and arguments. The second string manipulation layer can then be applied to a single command or an entire script. Finally, I will demonstrate several techniques for content execution using PowerShell command input parameters that hide command line arguments from appearing for powershell.exe.

Attempting to detect every possible obfuscated version of particular commands is not an efficient means of detection. Updated PowerShell event logging mitigates many of the detection challenges that obfuscation introduces. However, many organizations do not enable this PowerShell logging and rely primarily on command line logging. Therefore, I will provide techniques that the Blue Team can use to detect the presence of these obfuscation methods in command line arguments. I will also highlight methods using C# within powershell.exe that enable the attacker to execute .Net functions without being recorded in PowerShell event logs.

Attackers and popular frameworks like Metasploit, PowerSploit, and Empire use PowerShell's remote download cradle to execute remote scripts on a target system entirely in memory. This capability is typically used to avoid A/V and many application whitelisting products. I will give particular focus to the numerous ways within PowerShell, .Net, and native Windows applications that this remote

download functionality can be accomplished without using .Net's popular Net.WebClient class. I will also explore a half dozen functions that attackers can use to encode and decode PowerShell commands, including .Net's SecureString functions.

I will conclude this talk by highlighting the public release of Invoke-Obfuscation.ps1. This tool applies the aforementioned obfuscation techniques to user-provided commands and scripts to evade command line argument detection mechanisms. These techniques are available as miniature plug-n-play versions to be easily added to existing PowerShell frameworks in an effort to promote more wide-scale adoption.

Mobile Device Forensics – *Dav Wilson - @dav92178*

With digital devices being involved in an increasing number, and type, of crimes the trace data left on electronic media can play a vital part in the investigation process.

Hashview, a new tool aimed to improve your password cracking endeavors.– *Casey Cammilleri - @caseycammilleri and Hans Lakhan - @jarsnah12*

As penetration testers we crack passwords all the time. Usually doing the same tasks over and over. Hashview is a new open source tool debuting at Derbycon. It aims to optimize your workflow using a web front-end to leverage hashcat. Our team needed a tool that was geared toward consultants. This means solving the following everyday challenges: Not sending your client's hashes to foreign services, job management, analytics worthy of going directly into your reports, reusing and synchronizing previously cracked passwords, optimizing your dictionaries and masks, improving your utilization by always making sure jobs are running. Hashview aims to solve these issues while saving you time and improving your quality of reports.

Hardware Hacking the Easyware Way – *Brian Fehrman - @fullmetalcache*

Interested in hardware hacking but not quite sure where to start? Does the thought of soldering thrill you (or scare you)? Come check out this talk to see just how easy it is to jump into this exciting field of research!

Many people and companies use similar models of hardware. Unlike software, these devices rarely receive security updates. Sometimes, used devices are sold without clearing the configurations and important data is left behind. After this talk, you will know how to find hidden interfaces on these devices, start searching for vulnerabilities and sensitive information, and have irresistible urges to go home and tear apart all your old networking equipment. Did we mention… live demo?

1:00pm–1:50pm

MariaDB: Lock it down like a chastity belt – *Ben Stillman*

A general overview of some steps you can take to help secure your MariaDB database.

IoT Defenses - Software, Hardware, Wireless and Cloud – *Aaron Guzman - @scriptingxss*

The vast playground of IoT, and all its problems, will surely transfer from Consumer homes over to the Enterprise. Various studies have shown the effect of consumer IoT adoption in the enterprise, resulting in rouge connections into a trusted network. Items such as Smart TVs, drones, home security devices, and even connected vehicles are now being discovered in corporate networks. Industry professionals and board rooms are struggling to keep up with the growth of IoT due to the various interfaces introduced. We will discuss the many IoT attack surfaces and provide proactive security controls that are easily implemented by consumers, enterprises, and manufactures alike.

Static PIE: How and Why – *Adam Cammack and Brent Cook - @busterbcook*

Self-relocating executables without external dependencies (static PIE) have been an area of interest in embedded systems and defensive security research inside OpenBSD. We will explore how to create these binaries, how they are currently being used in defensive security, and novel offensive applications involving code execution in highly restricted environments. We will then demonstrate a new Metasploit payload that reflectively injects itself into running Linux processes.

Finding a Weak Link: Attacking Windows OEM Kernel Drivers – *Braden Hollembaek - @bhollemb and Adam Pond - @pondsploit*

The security of OEM drivers is an oft-overlooked blind spot that serves to undermine platform hardening efforts. To show that the rigorous security development lifecycle applied to Microsoft developed software does not extend to the OEM developers that bundle kernel drivers in with their hardware, we developed tools, methods, and techniques to efficiently produce exploitable kernel driver vulnerabilities in our fully patched Windows 10 installations.

This talk will dive into the methodology and tools we created as well as the vulnerabilities we found during this investigation. We will take a close look at effective driver fuzzing and how modifications we made to a public fuzzing tool resulted in exploitable crashes. We introduce and demo our new IDA Pro plugin, DriverBuddy, that automates much of the repetitive tedium involved with kernel driver reverse engineering. We will then discuss vulnerability analysis techniques, such as the efficient triaging of crash dumps and patterns of exploitability. Finally, we will discuss the results of our methods by analyzing some of the vulnerabilities we discovered and deep-diving an exploit against our Windows 10 laptops that allows us to map and read physical memory, including the kernel memory containing the Bitlocker AES key, as an unprivileged user.

FRIDAY – 9.23.

12:00pm–12:25pm

Go with the Flow: Get Started with Flow Analysis Quickly and Cheaply – *Jason Smith - @automayt*

Some people love buzzwords. I hate them personally. This is especially true for zazzy terms that describe things people have been doing or dealing with for ages. This talk will focus on setting up a next generation platform that will allow you to take control of big data, and hone your hunting skills at the same time. I'm kidding. Whats old is new again, so we're diving into some network flow data. I'll show you how to set it up quickly (less than 10 minutes) and for free (hardware not included). I'll also be showing you how to get started with analysis using some common and not-so-common situations.

12:30pm–12:55pm

Abusing RTF: Exploitation, Evasion and Exfiltration – *JDevon Greene - @DasMe_Devon*

If you knew how many ways you could obfuscate and deliver payloads with RTF documents, you would have thought it was a file format Microsoft secretively purchased from Adobe. 2016 has peeked my interest in the RTF specification, come learn why. This talk walks through examples that abuse the RTF specification and address these 3 key areas with RTF documents: Exploitation, Evasion and Exfiltration.

Audience members will gain a technical understanding of: How this file format type is being leveraged in attacks today; Many ways RTF documents can be obfuscated to bypass security technologies; Ex-filtrate data in plain sight.

So come check it out! I've got evasions so effective -- it'll make you wanna slap yo' mama!

1:00pm–1:25pm

Information Security Proposed Solutions Series - 1. Talent – *JAaron Lafferty - @zenrandom*

Have you ever noticed that when you get outside of the technical presentations at information security related talks that solutions are rare? Sure, we do a great job of; finding the problem, explaining the problem, then echoing that problem for literally years. However, we rarely get around to proposing a solution, much less attempting one. In this talk we will take time to probe elements of the shortage and recruitment of talent issue and discuss a proposed solution and it's effects. These may not be "the answers" but their at least something to try!

1:30pm–1:55pm

DNSSUX: Why DNSSEC Makes Us Weaker – *JAlfredo Ramirez - @bonds0097*

The DNSSEC specification was released in 2005 to help secure our DNS infrastructure and protect domains from being spoofed by implementing a PKI similar to what is used for SSL Certificates. Fast-forward to now and everyone is using it, right? Wrong. Not only are less than 1% of major websites using DNSSEC, but those that are arguably weaken their security posture by exposing all of their domains to reconnaissance by bad actors. In this talk we will walk through the history of DNSSEC, why its adoption has stalled, weaknesses in the spec and what we can learn to help build better systems to protect our DNS.

2:00pm–2:25pm

Nose Breathing 101: A Guide to Infosec Interviewing – *wartortell - @wartortell , Aaron Bayles - @AlxRogan*

The Information Security sector is a special place filled with special snowflakes. For a special snowflake, interviewing for a job can sometimes be a daunting or awkward task. There is a thin line when talking to humans between looking cocky and potato. On the other side, the interviewer must understand that there's a limited pool of special snowflakes. There's a sweet spot between auto-hiring someone and telling them you'll need three months to make a decision. Each snowflake must be nurtured into a beautiful snowerfly, or whatever their final form may be.

For this talk I plan to start a conversation about how to interview and be interviewed in the information security space. Good interviews combine a mix of targeted questions, appropriate information sharing, and a goal of what you'd like to learn from a person and vice versa. Bad interviews… don't. This leads to bad hires, good snowflakes being pushed aside, stupid questions being asked, people being sad pandas, poor team cohesion, and a general overwhelming feeling of meh. Do not despair, this is a solvable situation. Come join me on the journey to being less meh at hiring!

2:30pm–2:55pm

Android Patchwork: Convincing Apps to Do What You Want Them To – *William McLaughlin*

For better or worse, Java applications are all over the place. Our favorite cross-platform nightmare can be seen basically everywhere, powering all types of software. We can observe it in the wild running at the heart of an Android application, acting as the backend of a web application, and sometimes even pretending to be a desktop application.

The popularity of Java means we, as security professionals, need to be able to understand and dissect Java applications effectively. An essential tool in accomplishing this is a powerful debugger. When it comes to Java, many Integrated

Development Environments (IDEs) come bundled with a debugger. These include Netbeans, Eclipse, and IntelliJ IDEA.

However, a command line user will find options limited. A popular choice is jdb, the Java DeBugger. jdb is a command line debugger created as a demonstration of the Java Platform Debugger Architecture (JPDA). Basically, it's a proof of concept that has kinda become the standard for command line Java debugging.

This isn't ideal. As such, I've set out to make a better Java debugger. Starting where Oracle left off, I have been aiming to bring jdb up to the level of other powerful debuggers by implementing some much needed functionality. Functionality such as command history, tab completion, more intuitive keybindings, and various other features suggested by fellow security professionals. This talk focuses on my work so far, and my continuing work, on the path to making the jdb dream come true.

3:00pm–3:25pm

Is that a penguin in my Windows? – *Spencer McIntyre - @zeroSteiner*

One of the latest features coming out in Windows is the new Windows Subsystem for Linux. This brand new system provides translations for Linux syscalls via a new kernel interface. This talk will go over the technical details of this brand new interface with a focus on it's security implications. We'll go over features that might be beneficial to be leveraged by pentesters as well as what how the new subsystem can be abused by local exploits targeting Windows.

3:30pm–3:55pm

Real World Attacks VS Check-box Security – *Brent White - @brentwdesign and Tim Roberts - @zanshinh4x*

When scoping a penetration test for a client, there is often a disconnect between "check-box" requirements and actual preparation for what real-world attackers might attempt. With an influx of major data breaches, organizations need to take ownership and realize that compliance is not a "silver bullet" and is subject to the implementation of the organization's needs and requirements.

Check-box security isn't a bad start, but it's just that--a start. Because it's often required for compliance, it seems to be the main, or only driver for many security programs. This pushes companies to just meet the minimum requirements, can instill a false sense of security and can overshadow the entire view of their security posture.

This talk will cover what we often see as pentesters in regards to scoping an assessment with a client and views/ways to help them broaden their understanding of attack methods that go far beyond the requirements of "check-box security" to hopefully help improve their security posture overall.

4:00pm–4:25pm

ARRR Maties! A map to the legal hack-back – *Natalie Vanatta - @natalie_vanatta*

Defense of the nation (and by extension its citizens) is the only task that the Constitution tells the federal government that it must do. But, what happens when the government is ill-equipped to handle the defense? Today, we are bombarded by both nation-state and non-state actors operating within cyberspace with the goal to steal our property, harm our livelihoods, and destroy our way of life.

In the early days of the nation, we faced a similar dilemma on the high seas which resulted in the issuance of letters of marquis & reprisal to private citizens and corporations. Our government could not field and maintain a naval force that could defend the nation and its citizens. This talk will draw parallels between the nation's situation then and our situation today with respect to cyber security. Utilizing legal statues and lessons learned over the last two hundred years, I will propose a methodology that enables private groups to petition for the right to become privateers (aka patriots) and "hack back" their foreign attackers.

4:30pm–4:55pm

Project MVP - Hacking and Protecting SharePoint – *Michael Wharton - @MyProjectExpert*

SharePoint has become one of the fundamental building block for many business. Designed primary for managing documents and facilitation communication and collaboration within an organization, it can also become a big security hole in organization when not setup properly. The presentation goes of some of the basics of SharePoint, tools for exploiting SharePoint and what you can do to close the exploits.

5:00pm–5:25pm

Responder for Purple Teams – *Kevin Gennuso - @kevvyg*

This talk will focus on the tool Responder and how it can be used by both attackers as well as defenders. We'll review the current feature set, other tools that work in conjunction with it, and demonstrate its use in real-world scenarios for penetration testers and blue teamers alike.

5:30pm–5:55pm

Metaprogramming in Ruby and doing it wrong. – *Ken Toler - @relotnek*

Ruby is a powerful programming language, it includes way to write dynamic code at run time, this is called meta-programming. Meta-programming, everyones favorite Rubyism to hate. It can lead to less code, more abstraction and tears of pain and sorrow. During the review of lots of Rails and Ruby applications we've see how meta-programming has lead to some really interesting but terrible security flaws.

In this talk, we'll do a deep dive into examples of how meta-programming can bite you in a big way.

6:00pm–6:25pm

Evolving your Office's Security Culture – *Nancy Snoke - @NancySnoke*

Every work place has its own security culture defined by the values, traditions, beliefs, interactions, behaviors, and attitudes of the group. Many companies have appropriately stated security policies and standards that are not reflected in practice due to the security culture of the office, or it is difficult to change the policies and standards due to the security culture. In this talk I discuss how to stimulate change in an organization. I will go through multiple real life situations and discuss my successes and failures to stimulate change.

Some of the real life situations include getting the business to change requirements that are not secure, improving the level of security awareness in IT staff / programmers / code, changing security policies that hurt overall security, and more. I have statistical data on the efficacy of some of the methods discussed, and go through a post mortem on the failures to help others avoid the same mistakes.

6:30pm–6:55pm

Confronting Obesity in Infosec – *Michael Schearer - @theprez98*

Take a look around you at any con and you'll likely see the problem right before your eyes: our industry has an obesity problem. The numbers back it up, too: those who work in office environments (as many of us do) are more obese, exercise less, and suffer pay discrimination. Many travel a lot and live out of a suitcase. Our meals come from airports and fast-food restaurants. Who has time left over for the gym? Add to that the hidden health dangers of obesity and you have a recipe for disaster. Whether you're obese (like I was) or not, you can learn something from this rant: our community is the biggest support group you'll ever have to get yourself on the right track. I'll share my personal story as an example of what you can do. It's time we come together as a community to help fight this problem. Won't you join us?

7:00pm–7:25pm

BurpSmartBuster - A smart way to find hidden treasures – *Patrick Mathieu - @Pathetiq*

Bruteforcing non-indexed data is often use to discover hidden files and directories which can lead to information disclosure or even a system compromise when a backup file is found. This bruteforce technique is still useful today, but the tools are lacking the application context and aren't using any smart behaviour to reduce the bruteforce scanning time or even be stealthier. BurpSmartBuster, a Burp Suite Plugin offers to use the application context and add the smart into the Buster!

This 20 minute presentation will reveal this new open-source plugin and will show practical case of how you can use this new tool to accelerate your Web pentest to find hidden treasures! The following will be covered:

- How to add context to a web bruteforce tool
- How we can be stealthier
- How to limit the number of requests: Focus only on what is the most critical
- Show how simple the code is and how you can help to make it even better!

7:30pm–7:55pm

Advanced Persistent Thirst (APT) – *Patrick DeSantis- @pat_r10t, Joe Marshall - @ImmortanJo3 and Carlos Pacho- @CarlosMPacho*

Advanced Persistent Thirst (APT) is project to convert a refrigeration and cooling device (refrigerator), customized to cool and dispense liquids from a barrel-shaped metallic storage container (keg), and augmented with the power and magic of ICS/SCADA. APT takes a kegerator and adds physical and logical controls via industry standard hardware, software, and protocols, to manage (control and/or restrict) the process of dispensing beer. A 'real world' industrial programmable logic controller (PLC) handles the automated controls while a touchscreen interface is implement for normal user interaction. After the talk and demo, attendees will be invited to connect to the APT network and 'hack for beer'.

SATURDAY – 9.24.

9:00am–9:25am

We're a Shooting Gallery, Now What? – *Joseph Tegg - @AvgJoeSecurity*

The Red Team / Pentest Team just handed our CISO a report that says the network is a "Shooting Gallery". Sure, we test, just like everyone else. We use internal or 3rd party pentest / red teams to evaluate our security controls and policies in an effort to reduce the risk exposure, and the results are always the same. This discussion will shine the light on one of the often overlooked critical processes in a mature vulnerability management program: looking past individual findings to discover root causes and address the true systemic problems that make the enterprise network a perennial shooting gallery.

9:30am–9:55am

Malicious Office Doc Analysis for EVERY-ONE! – *Doug Burns - @dougsec*

Are you analyzing malicious office documents that your users dutifully send to you daily, or are you satisfied with just throwing it on VirusTotal and hoping for the best? In this talk I'll discuss why you should be manually analyzing ALL documents that make it through your email filters. You don't need a full time malware analyst to just do some cursory investigation. In this talk I'll show you how to analyze malicious office docs so you can quickly triage the threat. Are you blocking the delivery URLs? Does your A/V detect the second stage? Was this a targeted attack to your organization or just a shotgun blast that you got caught in? I will present a methodology for getting quick information from the document, share some tools I've found which make the job easier, and introduce some quick wins to decrease your overall malware volume.

10:00am–10:25am

The 1337 Gods of Geek Mythology – *Justin Herman - @JDogHerman and Anna-Jeannine Herman - @DJAJ9*

Join me in a look back though popular culture. We will be looking at the history of hacking and the public's perception though the lens of entertainment.

10:30am–10:55am

Open Source Intelligence- What I learned by being an OSINT creeper – *Josh Huff - @baywolf88*

Open Source Intelligence or OSINT is an incredible tool when it comes to reconnaissance. Its uses come in many varieties and the information obtained can be nothing short of scary if you know how to do it right. This talk covers defining OSINT, OSINT exercises, current tools, lessons learned in studying OSINT(which apply to many other security disciplines), some leaders in OSINT research and how studying OSINT helped me break into the information security job industry.

12:00pm–12:25pm

Finding Your Balance – *Joey Maresca - @lOstknOwledge*

Many people feel like the information security field and the vast growth it has seen over the last few years is unsustainable. They may very well be right; however, there is something far worse that may kill off the industry, and it is ambivalence of security as a whole.

In trying to make many of the arguments for improved security and for strengthening ourselves against attacks, have we only created a de-sensitization effect where the users and industries now just assume the risk and don't take the threats seriously. If eventually no one cares, then what does it mean for an entire industry? Can we even do anything to fix it, or have things already gone too far?

12:30pm–12:55pm

Hashcat State of the Union – *EvilMog - @EvilMog*

*Hashcat has changed a lot in the last year, this talk will outline the changes, give an overview of the roadmap, and give reasonings behind why *hashcat went open source.

1:00pm–1:25pm

Establishing A Foothold With JavaScript – *Casey Smith - @subTee*

Yes, you read that right. JavaScript is everywhere, and is often overlooked. This talk will briefly outline some tactics you can use to establish a foothold and persist in an Enterprise network using only JavaScript. I will demonstrate some fileless persistence mechanisms.

1:30pm–1:55pm

Overcoming Imposter Syndrome (even if you're totally faking it) – *Jesika McEvoy - @octalpus*

Imposter Syndrome has been oft discussed in the context of gender or other minorities and mentoring, but these discussions have left out the greater truth – nearly everyone in the infosec community experiences this phenomenon. This talk is designed to approach the topic from a broader perspective. It will contain tips on not only overcoming this ourselves, but how to use this confidence to be a mentor and role model to others. This talk highlights the challenge current and emerging researchers encounter – feeling supported in pursuing a research path and speaking authoritatively when the cutting edge nature of infosec is counterproductive to building confidence in your own expertise. If we want to continue to be a research-focused community, we need to address some of the underlying issues that are contributing to the stagnation and drain of the brain trust.

2:00pm–2:25pm

Security v. Ops: Bridging the Gap – *Craig Bowser - @reswob10*

For years the security industry has talked about how hard it is to communicate and work with users. But what about the relationship between security and operations? How is your relationship with Ops? Do you have a solid partnership or do you only talk when absolutely necessary? How much is the security of your enterprise helped by cooperation or hurt by the lack thereof? Is it possible to have a fully OPERATIONALLY SECURE network without these two groups working well together?

Unfortunately, these two groups usually are in opposition to each other, with each side complaining that the other doesn't know what they are doing, doesn't understand what's important, and doesn't know how to run a network. This presentation will discuss the reasons for some of the biggest sources of friction and provide suggestions for resolution. If the gap between these two groups can be bridged, it will increase our ability to provide our customers and our users a secure environment to interact with, work in, and develop for so they can accomplish their mission.

2:30pm–2:55pm

From Gaming to Hacking The Planet – *Chris "Lopi" Spehn - @_Lopi_*

Have you ever wondered if all that time you spend playing games is a waste? I'm here to tell you it's not a waste. Without gaming, I wouldn't be where I am today. Gaming taught me how to think creatively, gaming taught me how fuzz all things, and most important; gaming taught me how to hack the planet. We will explore how gaming helped get me where I am today, why you should keep gaming, and how you can start applying what you've learned from playing games directly to information technology and security. If you're lucky, you might even see a demo of the educational game I've been developing; possibly even play it!

3:00pm–3:25pm

SQL Server Hacking on Scale using PowerShell – *Scott Sutherland - @_nullbind*

This presentation will provide an overview of common SQL Server discovery, privilege escalation, persistence, and data targeting techniques. Techniques will be shared for escalating privileges on SQL Server and associated Active Directory domains. Finally we'll show how PowerShell automation can be used to execute the SQL Server attacks on scale. All scripts created and demonstrated during the presentation will be open sourced. This should be useful to penetration testers and system administrators trying to gain a better understanding of their SQL Server attack surface and how it can be exploited.

3:30pm–3:55pm

Dive into DSL: Digital Response Analysis with Elasticsearch – *Brian Marks - @brianDFIR and Andrea Sancho Silgado*

In this talk we will take a deep dive into the Elasticsearch DSL using python and how you can use it to go beyond the simple searches you may have been using in Kibana. We will demonstrate how Elasticsearch can be used to speed up and automate your DFIR investigations by grouping multiple queries of artifacts into a "signature of forensics" format to answer common investigator questions. In addition, this talk will explore the full power of elasticsearch's searching and aggregation capabilities that can be utilized with indexed artifacts as well as the visualization functionality of Kibana.

Use cases and code samples from real world investigations will be presented showing how you tap into this functionality already built into your ELK stack!

4:00pm–4:25pm

Making Our Profession More Professional – *Bill Gardner - @oncee*

If information security professional are going to be taken seriously about the organizations we server we need to become more professional. There are many way of achieving this goal but it's going to take culture change in our community. This talk will define this problem and offer some solutions on how to work toward solving this problem.

4:30pm–4:55pm

How are tickets paid for? – ***Abe Miller****

I don't have company CC, and not sure what options I'll have on Sunday… plus it'd help my teammates - all of us have to pay out of pocket (initially). Just a guy looking for an answer to a question… Sorry - there was no 'contact us' page for questions.

5:00pm–5:25pm

Security Automation in your Continuous Integration Pipeline – *Jimmy Byrd - @jimmy_byrd*

Developers use unit tests and acceptances tests in continuous integration (CI) to find bugs early and often in a repeatable way. Security is an important part of any software development life cycle. So why not add security analysis tools to this pipeline? This talk will cover adding and using OWASP/ pipeline, a framework made for running security analysis tools in CI.

5:30pm–5:55pm

"Cruise Ship Security OR Hacking the High Seas – *Chad M. Dewey - @chaddewey*

Taking a cruise vacation should be a laid back, care-free endeavor that allows one to unwind, have a few drinks, explore new countries, and get sunburned. For many, there is not much thought put in to how the cruise ships operate or how secure your stored information is on the ship. After all - you're on vacation. In this presentation, three leading cruise lines have been evaluated in several different security realms over the last 10 years. These areas include physical security, social engineering, wifi vulnerabilities, segregation of passenger network from operations network, financial transactions, information sanitization, and more. Some vulnerabilities are simple hacks to allow one to obtain free wifi, while others are more complex and allow one to explore the ship in more obscure ways. In this presentation, successes and failures of hacking the high seas will be shown.

6:00pm–6:25pm

Web Security for Dummies – *Lee Neely - @lelandneely*

Today's web surfing experience is more riddled with landmines than ever, which results in compromises of end-user systems by the use of perpetually insecure browsers, plugins, and sometimes just bad user behavior. A few changes to approaching how you surf the web can raise the bar on the risks to compromise, such as using TOR, removing Flash and Java, and more.

Additionally, many of us run or validate the security of web servers. There are a few things web server owners can do that also aid users with a secure browsing experience. More and more users are looking for these same security enhancements, and such as the ISRG Lets Encrypt project's free SSL/TLS certificates.

This discussion will give you a short list of changes to better secure the web surfing experience both for users and customers.

After completing this session, participants will be able to:
1) Learn some optimal browser configuration options
2) Learn some browser best practices
3) Learn some web server configuration best practices
4) Learn about The Onion Network (TOR)
5) Learn about free HTTPS certificates for Web Servers.

6:30pm–6:55pm

I Love myBFF (Brute Force Framework) – *Kirk Hayes - @kirkphayes*

This presentation will feature the release of a new open source tool which combines fingerprinting and brute forcing against some common web applications, including Citrix, HP, Juniper, and MobileIron, to add intelligence to password guessing. Better yet, this tool is modular, allowing the easy expansion of the tool to include not only other web applications, but also other services. We will look at different password guessing techniques, their shortcomings, and how myBFF can address these shortcomings. The best part is that the tool will do more than just tell you if a credential pair is valid! You don't want to miss this!

7:00pm–7:25pm

Nobody gets fired by choosing IBM… but maybe they should. – *Cameron Craig and Keith Conway - @algirhythm*

This talk explores how to positively influence monolithic corporations towards collective action. Compared to the typical infosec environment, our process leverages a slightly unorthodox yet effective application of social engineering, red teaming and design thinking. The goal of this presentation is to outline a practical approach by exploring four main vectors: people, environment, timing and message. Leveraging the techniques in this talk, viewers should be empowered to pivot corporate strategies, solve unmet customers needs simply and simultaneously build a great company.

7:30pm–7:55pm

Shackles, Shims, and Shivs - Understanding Bypass Techniques – *@Mirovengi*

Our industry recognizes the importance of physical security, but often, we focus on the lock core itself and the challenges with picking it. This talk discusses an overview of the common retention mechanisms and how many of the common forms can be bypassed quicker than picking the lock.

SUNDAY – 9.25.

10:00am–10:25am

Abusing Linux Trust Relationships: Authentication Back Alleys and Forgotten Features – *Ronnie Flathers - @ropnop*

Passwords are weak, and generally speaking, the less a company relies on them, the better. Instead of using password authentication for multiple services and sending passwords (or hashes) all over the network, companies have started trying to adopt more password-less authentication mechanisms to secure their infrastructure. From SSH bastion hosts to Kerberos and 2FA, there are many controls that attempt to limit attacker mobility in the event that a single account or password is compromised. This session will be a "walking tour" of bypass techniques that allow a small compromise to pivot widely and undetectably across a network using and abusing built in authentication features and common tools.

Starting with a simple compromise of an unprivileged account (e.g. through phishing), this session will discuss techniques that pentesters (and real world attackers) use to gain footholds in networks and abuse trust relationships in shared computing resources and "jumphosts". The session will demo common tricks to elevate privileges, impersonate other users, steal additional credentials, and pivot around networks using SSH. The presentation will culminate with a discussion of 2FA for SSH access, and how compromises elsewhere in a network can be exploited to completely bypass it. Since these tricks and techniques utilize only built-in Linux commands, they are extremely difficult to detect as they look like normal usage.

The demo environment will mimic a segmented network that uses Kerberos and two-factor authentication on SSH jump hosts. It is based entirely off real-world experiences and setups that pentesters in Cisco's Security Services have encountered.

10:30am–10:55am

Samsung Pay: Tokenized Numbers, Flaws and Issues – *Salvador Mendoza - @netxing*

Samsung announced many layers of security to its Pay app. Without storing or sharing any type of user's credit card information, Samsung Pay is trying to become one of the securest approaches offering functionality and simplicity for its customers.

This app is a complex mechanism which has some limitations relating security. Using random tokenize numbers and implementing Magnetic Secure Transmission (MST) technology, which do not guarantee that every token generated with Samsung Pay would be applied to make a purchase with the same Samsung device. That means that an attacker could steal a token from a Samsung phone and use it without restrictions on other devices.

Inconvenient but practical is that Samsung's users could utilize the app in airplane mode. This makes impossible for Samsung Pay to have a full control process of the tokens pile. Even when the tokens have their own restrictions, the tokenization process gets weaker after the app generates the first token relating a specific card.

How random is a Spay tokenized number? It is really necessary to understand how the tokens heretically share similarities in the generation process, and how this affect the end users' security.

What are the odds to guess the next tokenized number knowing the previous one?

11:00am–11:25am

Fire Away! Sinking the Next Gen Firewall – *Russell Butturini - @tcstoolhax0r*

Recently, the next generation or "application aware" firewall has come onto the scene as the next logical progression of firewall technology and the platform of choice for enterprise traffic filtering needs. However, many vendors have overstated the capabilities of these firewalls and how the underlying technology really works. This talk will examine how next generation firewalls make decisions and how application awareness works, and then dive into the security tradeoffs they make in the name of performance. A new tool, Fireaway, will be demoed to show how the techniques covered in this talk can be automated to completely bypass firewall rules, exfiltrate data and establish obfuscated command and control channels through the firewall, all while looking like normal user activity.

12:00am–12:25am

PacketKO - Data Exfiltration Via Port Knocking – *Matthew Lichtenberger - @JousterL*

The art of data exfiltration is in getting the goods past security, both digital and analog. There are a myriad of ways to do this, but most involve in-channel methods of obfuscation. This talk will describe a method developed to break out of that paradigm, by using packet metadata to transmit the data. It will include a live demo of the operating software.

12:30am–12:55am

Ransomware: An overview – *Jamie Murdock - @b0dach*

This talk will cover the most common ransomware and a synopsis of how they operate, the different platforms, and the variants built off of these platforms.

1:00am–1:25am

The Beginner's Guide to ICS: How to Never Sleep Soundly Again – *Dan Bougere - @Rouxgaru*

Are you tired of missing the Modbus? Do you think DALI is a weird artist? You want to bring sexy BAC? Go from noob to clueful on the hottest new hacking targets of 2016, and see what all the fuss is about. Learn what exactly is SCADA/ICS, why it's important, and just how horrifyingly ancient it all is. If you've ever wondered why Stuxnet was so devastatingly effective, or want to lose sleep over chemical plants on your commute this is your chance.

“#MakeNetworkSecurityGreatAgain”

“Network Security
Beyond the Basics”

“You Wouldn’t Trust
An Out-of-Band Firewall”

“One box to rule them all
One box to find them
One box to inspect them all
and in the VLANs bind them”

“Security Beyond
the Firewall”

“It’s what’s on the
inside that counts”

www.miltonsecurity.com
261 East Imperial Highway, Suite 550, Fullerton, CA 92835 • tel: 1.888.674.9001 • fax: 1.714.459.7489

SPONSORS

DIAMOND

milton security

PLATINUM

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

GOLD

TrustedSec
INFORMATION SECURITY MADE SIMPLE

RISKIQ

BDS
BINARY DEFENSE SYSTEMS

L.J.KUSHNER
& Associates, L.L.C.

RAPID7

BOMGAR

CloudPassage

PLURALSIGHT

PWNIE EXPRESS

SecureIdeas
professionally evil

Symantec

vmware

SILVER

NinjaJobs.org
trusted · vetted · discreet

Malwarebytes

WarCollar
industries

SANS

CYBRScore

RENDITION INFOSEC
Security by any legal means

resilient
an IBM Company

Centrify

Stealthcare
CYBER INTELLIGENCE

MARSHALL
DIGITAL FORENSICS
INFORMATION ASSURANCE

BRONZE

PARTY

CTF

COFFEE

LogRhythm
The Security Intelligence Company

VENDORS

Social-Engineer
Black Hills Information Security
Hacker Stickers
Hacker Warehouse
Ace Hackware
The Security Awareness Company
No Starch Press
Hackers For Charity
Hak5

COBALT STRIKE

ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

Cobalt Strike is a platform for **Red Team Operations** and **Adversary Simulations**. If you like covert comms, scripting, pivoting, and post-exploitation--you should stop by our table. We're fun! Really.

A Special Thank You to our Trainers:

Carlos Perez and Jose Quiñones
Mick Douglas and Adam Crompton
Paul Koblitz and Larry Spohn
Deviant Ollam and Babak Javadi
Chris Hadnagy
Josh Stroschein
Tim Tomes
Dr. Jared DeMott
Matt Weeks
Jason Williams and Jack Mott
Kevin Johnson, Jason Wood, Jason Gillam
Kyle Wilhoit and Stephen Hilt
Tyler Hudak
Ryan Linn and Thomas McCarthy

We would like to express our most sincere gratitude
to everyone who volunteered their time in assisting us
in the very early mornings and the very late nights,
making DerbyCon run smoothly year after year.
Without your help and support,
this conference would not be as great as it is today.

- Dave K, Martin, Adrian, Erin, Paul, Dave D, and Karl

Tweets

THE CRYSTAL METHOD @crystalmethod
@Harvest, Louisville getting fueled up 4 #DerbyCon. R U ready?!!
28 Sep 2013

Jess @J3ssa
Hats off to @DerbyCon staff and volunteers. Very well run, great content, and I now know why it is loved by so many. Thanks to all!
29 Sep 2013

DerbyCon @DerbyCon
Quick factoid: we were only the @HyattLou 2nd highest bar sales on Saturday ever.. Only one to beat us was us on Friday. Wow #DerbyCon
29 Sep 2013

Walt Berstler @KingofBigWheels
@DerbyCon Raised it to a new level with Crystal Method. Amazing show. Thanks to everyone that helped out. #derbycon
29 Sep 2013

HyattLou @HyattLou
@DerbyCon We're still tallying the damage, but definitely one for the ages #challengecrushed #derbycon
29 Sep 2013

Space Rogue @spacerog
Proof that #derbycon owns Louisville, unsolicited ? from taxi driver "You're here for that convention right? Which Internet should I get?"
29 Sep 2013

HyattLou @HyattLou
Safe travels & many thanks, #Derbycon! U'r always one of our fav cons to host -- time to restock the fridge for next year!
29 Sep 2013

Razor @RazorEQX
#Derbycon My new immediate family in Louisville. I love you guys!! cc @essobi
29 Sep 2013

Joshua Corman @joshcorman
Wow! @irongeek_adc team are AMAZING! Tons of #DerbyCon video already online
1 Oct 2013

Katie Moussouris @k8em0
Thanks to all who made #DerbyCon such a brilliant collection of experiences. Great to join the family. :-)
1 Oct 2013

Ed Skoudis @edskoudis
I'd like to thank you again for hosting an AWESOME con. It was so family friendly, I just loved it! I'm now a HUGE DerbyCon fan.
24 Oct 2013

WWW.DERBYCON.COM