PROGRAM
2016

BSidesNash.org
@BSidesNash

BSides Mid-TN, Inc. is proud to present :

BSides Nashville 2016

On behalf of the Organizing Committee, volunteers, speakers, and sponsors, we are pleased to have you at BSides Nashville 2016. This is year three and we have a lot to offer.

First we would like to thank our sponsors. Without their generosity, this conference (and many others) would not exist. Each of our sponsors brings resources and enthusiasm to the event. A special thank you goes out to Lipscomb's College of Computing and Technology for providing the perfect space and atmosphere for a third year. We are all students of the security craft, and we welcome the new students and the more experienced to help us in our quest.

We want BSides Nashville to be more than talks and swag. We intentionally avoided tight schedules in the planning want to relax, share, and connect. We believe that the real value of a BSides is the community. You don't get to socialize when you race from room to room, trying to find a seat. So, find your slow, southern drawl (we will let you borrow one) and relax. Enjoy being with your like minded peers, discuss the latest project you are working on or pull up a comfy chair in the Phish Bowl and see what new things you can find.

Once again we are excited to bring you great speakers from around the United States and many from Tenneesee and nearby Kentucky. This year we were overwhelmed by the talk proposals and worked hard to pick a good variety to peak your interest in new topics or show a different way to look at issues we all know too well. Please show your appreciation, as they are volunteers and came at their own expense to share their knowledge.
Our special treat for you is the Phish Bowl, the area just around the corner where you will find a hacker playground. Who knows what we have cooked up for you this time.

Come see, meet, talk... and leave inspired.

Thank you for joining us and making it fun!
BSides Nashville Organizing Committee

We couldn't have done this without the help of our great organizing committee !

Lauren Rogers	**President**	**Adrian Crenshaw**	**Norse god & AV**
Geoff Collins	**Treasurer**	**RC**	**The Force**
Finn Breland	**Secretary**	**Jennifer Samardak**	**Nerf Herder**
Gabriel Bassett	**Badge Wrangler**	**Victor Wieczorek**	**Sponsorship team**
Tommy Wolosin	**Swagger Supplier & Sponsorship team**	**Jamin Smith**	**Community liaison and minion**
Lill Haber	**Decentralized Information Asset Instigator**	**Shelby Gray**	**Strategic Partnership Disruptor**
NSA_Key	**Phish the Hoopy Phrood**	**Scott Haber**	**Silent Partner**

Partner with Nashville's pacesetter in technology education.

MS-Information Technology

MS- Software Engineering

MS- Data Science

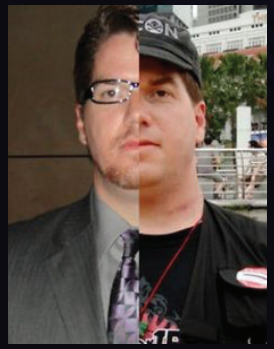
Whether you need to acquire new talent, create stronger employees or create your own impact in the IT community, Lipscomb University leads the way with innovative and one-of-a-kind graduate degrees for our region as well as industry partnership programs, community events and a strong commitment to developing tomorrow's leaders.

Find out what it means to have Lipscomb's College of Computing and Technology on your team. Contact Finn Breland at **finn.breland@lipscomb.edu** for more information.

LIPSCOMB UNIVERSITY | COLLEGE OF COMPUTING & TECHNOLOGY

technology.lipscomb.edu

KEYNOTE SPEAKER:



Jayson E. Street

@jaysonstreet

Jayson E. Street is an author of "Dissecting the hack: The F0rb1dd3n Network" from Syngress. Also creator of dissectingthehack.com He has also spoken at DEFCON, DerbyCon, UCON and at several other 'CONs and colleges on a variety of Information Security subjects. His life story can be found on Google under "Jayson E. Street" *He is a highly carbonated speaker who has partaken of Pizza from Beijing to Brazil. He does not expect anybody to still be reading this far but if they are please note he was chosen as one of Time's persons of the year for 2006.

Kevin Bottomley

@k3v_b0t

Kevin Bottomley is a Security Analyst on the OpenDNS Research team. Throughout the course of the day, Kevin undertakes roles from creating Security Threat Reports for existing and potential clients, working closely with the Customer Support Team, finding new threats and attacks, and devising tactics to track down and identify nefarious actors and malicious domains. Kevin earned an Associate in Science degree from City College of San Francisco in Computer Networking and Information Security, and has earned various certificates along the way.

Past talking events include BSidesSF 2015, BSidesLA 2015, NASA Ames Security Week, BSidesNYC 2016, and BSidesSF 2016

Marc Brawner

Marc Brawner is an Associate Managing Director with Kroll's Cyber Security and Investigations Practice. With over 16 years of experience in information security, Marc is an expert in the areas of cyber risk, data breach investigations, forensics, and incident response.

Marc has participated in hundreds of incident response, computer forensics, and risk assessment activities, implemented and managed enterprise technology solutions, led vendor and regulatory compliance programs, and developed effective security policies and procedures. He works closely with legal, HR, and compliance personnel at organizations worldwide to deliver significant value and savings through creative use of cyber security and forensic capabilities.

Mike Brancato
@meatballninja

Mike is a computer security professional and has an interest in embedded devices, industrial and control systems. He performs security assessments and penetration tests on a wide variety of devices and applications. Mike has a strong professional background in networking, previously managing a team of network engineers for a large healthcare payment processor.

Chris Carlis

Chris Carlis is a Principal Consultant on the Dell SecureWorks Red Team. An experienced penetration tester with over 10 years experience in the Information Security arena, Chris enjoys finding unconventional solutions to unconventional security challenges. Locally, Chris is a community organizer in the Chicago area and helps coordinates a number of monthly gatherings designed to connect like-minded information security professionals.

Frank Catucci
@en0f

Frank Catucci is currently the Director of Web Application Security for Qualys and a Chapter Leader for OWASP, among other things that he gets called. He has over 15 years experience in the Information Technology and Security field. Have no fear, he has multiple Novell certifications. He is a Hacker, Breaker, Builder, Fixer, Father, Farmer, and Husband. Frank also conducts security research, freelance penetration testing, and often speaks at information security conferences and events such as BSides, OWASP, ISSA, etc

TrustedSec
INFORMATION SECURITY MADE SIMPLE

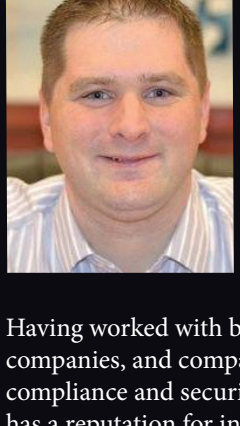
Lucie Hayward

Lucie Hayward is a CISSP and PMP certified project manager, specializing in project management and security. She is currently a Managing Consultant with the Cyber Investigations practice at Kroll in Nashville, TN. She assists clients in responding to cyber incidents, as well as creating Incident Response Plans and conducting Tabletop Exercises. She is a former ISSA and ISC2 board member, and is currently the 2015-2016 President of the PMI Nashville chapter.

Mark Heard

@tmdheard

Mark Heard is a native Tennessean who worked at Eastman Chemical Company in Kingsport, TN for over thirty years as a systems engineer. Mr. Heard has experience with a variety of Industrial Control Systems and applications and a continuing interest in computer and network technologies. He has been active in chemical sector Cybersecurity teams and in ISA99/ICE62443 standards working groups since 2002. Mr. Heard has also represented the chemical sector on the DHS Process Control Systems Forum and Industrial Control Systems Joint Working Group (ICSJWG) programs. He helped write the "Roadmap to Secure Control Systems in the Chemical Sector" and chartered the ACC Roadmap Implementation Working Group for that sector. Mr. Heard also spent a year in the IT Security Group at Eastman before joining Red Tiger Security to provide ICS cybersecurity assessment, consulting, and training. He currently represents integrator and consultant interests for the ICSJWG Steering Team and began working for Mandiant on the ICS Consulting team in 2015.



Chris Huntington

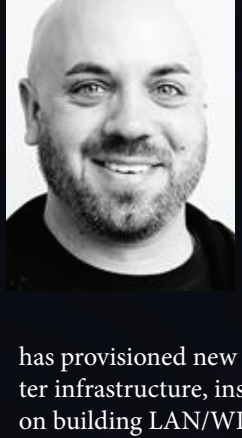
@linkstate

With over a decade in IT and Information Security, Chris is a security focused Solution Architect for Nexigen in Newport, KY. Having worked with banks, publicly traded companies, and companies with complex compliance and security requirements, Chris has a reputation for innovative designs and forward thinking security solutions.

Jeff Man

@MrJeffMan

Jeff Man is a Strategist and Security Evangelist at Tenable Network Security. He has over 30 years of experience working in all aspects of computer, network, and information security, including risk management, vulnerability analysis, compliance assessment, forensic analysis, and penetration testing. Early in his career, Jeff held security research, management and product development roles with the NSA, the DoD, and private-sector enterprises. Prior to joining Tenable, Jeff served as a QSA, first with TrustWave, then with VeriSign and finally AT&T Consulting Services. In this role he has provided PCI consulting and advisory services to many of the nation's best known brands.



Fletcher Munson

@Mr_FMunson

currently admins and maintains developer tools, ticketing systems, change and access control as well as all things linux on the enterprise side of the house. Previously, he has provisioned new network and datacenter infrastructure, installed and consulted on building LAN/WLAN/ACS systems and has held systems administration roles. Other machinations include network and application security, bluetooth and RFID lock research, lockpicking and other physical security as well as honing his personal protection skillset.

Ron Parker

@scmunk

Ron Parker is a senior security architect for Unum, the leading group and individual disability insurance provider. Ron has decades of experience successfully designing and developing secure application and infrastructure solutions in a complex and regulated environment. He has worked to implement security process improvements through establishing security frameworks and integrating security by applying architecture practices. He has been the architectural and technical lead for a large identity and access management solutions, service and API security, enterprise authentication/authorization frameworks, and various other systems that are required to secure any company. Ron is also a non-reluctant CISSP.

Evan Pena

@evan_Pena2003

Evan Pena is a Principal Consultant and Red Team lead for Mandiant's West Region. Evan has years of experience in enterprise information technology administration, leading covert red team operations to evaluate incident response procedures, and assessing enterprise network defense capabilities from the perspective of an attacker. In addition, Evan participates in security diverse assessments of large government agencies and Fortune 500 companies. These networks consist of an online presence of hundreds of thousands of address spaces around the world.

Tim Roberts

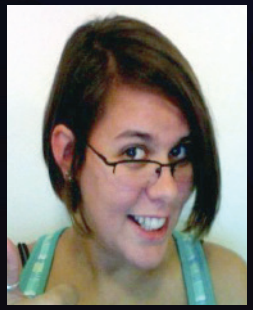
@ZanshinH4x

Tim is an Offensive Security Consultant within Solutionary's Professional Security Services Department (NTT Group Security Company). He is a nationally known speaker and has presented at Universities, BSides Nashville, CircleCityCon, DefCon 22 and the ISSA International conference. His experience includes Internal and External Penetration Assessments, Social Engineering and Physical Security Assessments, Wireless and Application Vulnerability Assessments, and more. Tim has held information and physical security as well as management roles across multiple industries, including healthcare and government. He has conducted highly successful Red Team Assessments.

Jason Smith

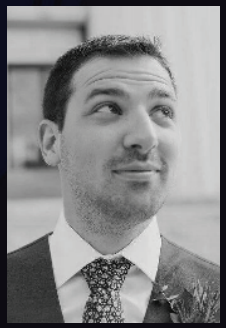
@automayt

Jason Smith has a background in physics and has built everything from particle accelerators to explosive neutralizing robots used by the military. He has worked in multiple US Department of Defense SOCs and was the lead security monitoring architect for the Commonwealth of Kentucky. Jason co-wrote Applied Network Security Monitoring and maintains the open source project FlowBAT, a graphical flow data analysis tool. Jason works remotely from his home in Bowling Green, KY and has been with FireEye since late 2013



Kate Vajda

Director of Customer Service for MiSec in Jackson, Michigan.
Kate currently does vulnerability management and pen testing for a utility company. Before working in security, she worked in IT as a network research manager and later moved to supporting SCADA systems. She has a passion for industrial control systems, her vice is redbull and her downfall is her willingness to help other people.



Jake Valletta

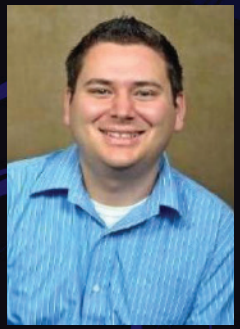
@jake_valletta

Jake Valletta is a senior consultant at Mandiant in San Francisco, CA. His areas of interest include mobile security, application security, penetration testing, and incident response. When not performing incident response and forensic services for fortune 500 and fortune 100 companies, he is likely working on improving and developing mobile testing tools or researching the AOSP project (or maybe just enjoying a craft beer). In his free time, he maintains a website and blog dedicated to mobile security and research called "The Cobra Den."

Jarred White

@eviljarred

Jarred is a security engineer with over a decade of offensive security experience, including social engineering and pentesting. He spends his free time using his security expertise to get free beer.



Christopher Truncer

@ChrisTruncer

Christopher Truncer is a red teamer with Mandiant. He is a co-founder and current developer of the Veil-Framework, a project aimed to bridge the gap between advanced red team and penetration testing toolsets. Chris began developing toolsets that are not only designed for the offensive community, but can also enhance the defensive community's ability to defend their network.

Johnny Xmas

@J0hnnyXm4s

Johnny Xmas is a penetration tester for RedLegg, based in Chicago, and has been speaking Internationally on the topics of Information Security, Career Advancement and Social Engineering for nearly 15 years, both in and very far outside of the Information Security community. His infamous mixture of humor, raw sincerity and honest love of people lead to hilarious, but at their core serious discussions revolving around his frustration over how much people seem to desire to get in their own way. Master of terrible accessorizing, you'll often find him mixing vests with wallet chains, man buns and bracelets, and almost invariably topping it all off with a pair of cat ears that have heard more than you'd ever want to know.

Wes Widner
@kai5263499

Wes Widner works at the intersection of big data and automated malware analysis. Wes has worked with threat intelligence at McAfee Lab's Global Threat Intelligence Group and Norse Corporation's Data Services group. Wes has a knack for getting vaguely defined projects off the ground and in that vein Wes has setup an automated malware analysis pipeline used to produce threat intelligence data from hundreds of thousands of malware samples received daily.

Brent White
@brentwdesign

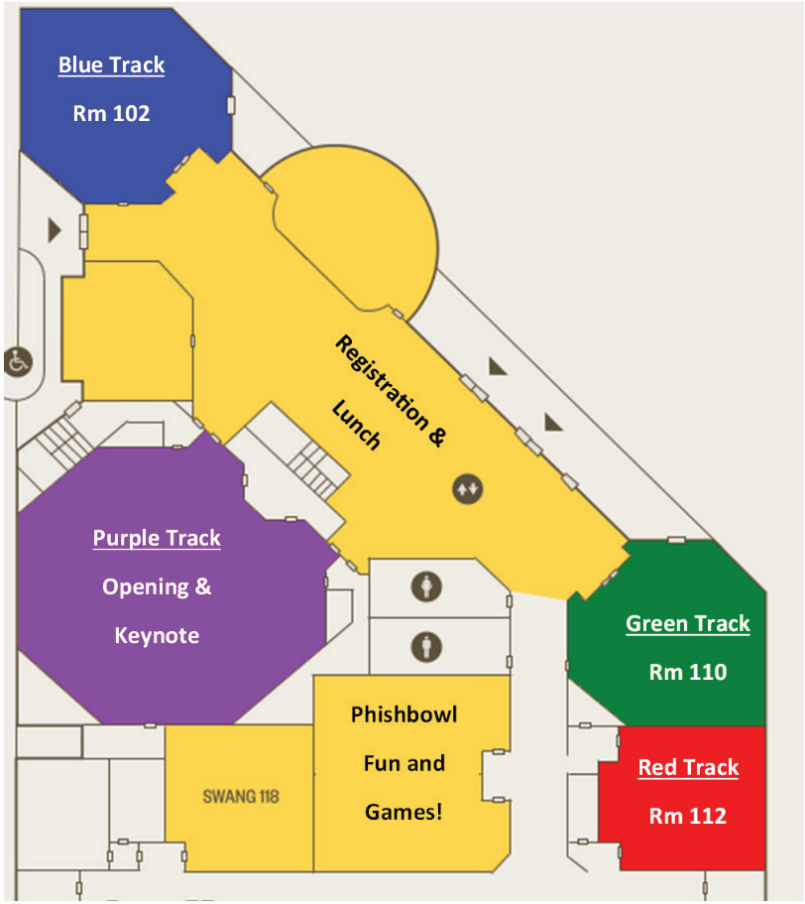
Brent is an Offensive Security Consultant at Solutionary--An NTT Group Security Company, and has spoken at numerous security conferences, including ISSA International, BSides Nashville, CircleCityCon, DEF CON 22 & 23, DerbyCon and more. He has held the role of Web/Project Manager and IT Security Director at the headquarters of a global franchise company. His experience includes Internal and External Penetration Assessments, Social Engineering and Physical Security Assessments, Wireless and Application Vulnerability Assessments, and more.

PUT YOUR NETWORK UNDER THE RELENTLESS GAZE OF QUALYS CONTINUOUS MONITORING

FOR A FREE TRIAL VISIT
QUALYS.COM/**CONTINUOUS**

QUALYS®

Get real-time alerts about potential vulnerabilities, so you can get on problems before hackers do. No manual deployment, no waiting for reports, all from the cloud.


Blue Track
Rm 102
Registration &
Lunch
Purple Track
Opening &
Keynote
Green Track
Rm 110
Phishbowl
Fun and
Games!
SWANG 118
Red Track
Rm 112

TIME	Purple : We're all in this together		
08:00 - 09:00	**REGISTRATION OPENS!!!**		
09:00 - 09:15	**Welcome to BSidesNashville**		
09:15 - 10:15	**Keynote: Jayson Street**		
10:15 - 10:30	**Coffee Break**		
Time	**Green**	**Red**	**Blue**
10:30 - 11:30	AppSec Enigma and Mirage - When Good Ideas Can Go Awry **Speaker: Frank Catucci**	Breaking Through Cellular Gateways and How I Gained Access to One of the US's Largest Energy Companies **Speaker : Mike Brancato**	At the mountains of malware. **Speaker:Wes Widner**
11:40 - 12:40	The Art of the Jedi Mind Trick **Speaker: Jeff Man**	Ever Present Persistence - Established Footholds Seen in the Wild **Speakers: Evan Pena, Chris Truncer**	Collection and Detection with Flow Data: A Follow Up **Speaker: Jason Smith**
13:00 - 14:00	**LUNCH sponsored by**		
14:00 - 15:00	How to get into ICS security **Speaker: Mark Heard**	Forging Your Identity: Credibility Beyond Words **Speakers: Tim Roberts, Brent White**	Container Chaos: Docker Security Container Auditing **Speaker: Chris Huntington**
15:10 - 16:10	The Ransomware Threat: Tracking the Digital Footprints **Speaker: Kevin Bottomley**	IAM Complicated: Why you need to know about Identity and Access Management **Speaker: Ron Parker**	It's Not If But When: How to Create Your Cyber Incident Response Plan **Speakers: Lucie Hayward, Marc Brawner**
16:20 - 17:20	InfoSecs in the City - Starting a Successful CitySec Meetup **Panel: J0hnny Xmas, Chris Carliss, Fletcher Munson, Kate Vajda**	Put a Sock(et) in it: Understanding and Attacking Sockets on Android **Speaker: Jake Valletta**	Threat Modeling the Minecraft Way **Speaker: Jarred White**
17:30 - 17:40	**Closing Ceremonies Sponsored**		
18:00 and Beyond	**After Party**		

Presentations

KEYNOTE SPEAKER:

…And bad mistakes… I've made a few…

Jayson E. Street

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 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 failures I've had in Blue Team, failures I've had in Red Team, and 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! ;-)

AppSec Enigma and Mirage – When Good Ideas Can Go Awry

Frank Catucci

The enigma of AppSec and the mirages of mitigating risk are something I often see in my day job as well as my personal experience and research.

An application looks secure; the developers had great intent, ideas and features. Follow through however, now that is a completely different story. I will demonstrate and walk through some valid cases in which the ideas of AppSec in a web app's design were valid and well thought out, however the execution of such security measures, not so much. The easy mistakes that can be made and the lack of testing often are the culprit. But sometimes, yeah, zero shits are given.
I will also address BugBounty programs. Some good, some not so much, and why. Finally I will offer advice on how to help progress and improve your AppSec programs. Thank you

The Art of the Jedi Mind Trick

Jeff Man

The hacker/security community continues to struggle with how to get our message across to others. We know what's wrong, what's insecure, and what needs to be done to fix the problems. BUT...we seem to hear more stories about failure rather than success stories. Maybe WE are part of the problem. It's easy to give a talk at a conference where you're "preaching to the choir" and everyone speaks your language, but how do you fare when you are trying to give the

message to your boss, or your boss's boss, or C-Level management?
This talk will explore a variety of techniques that I've learned over my 20+ years of consulting/advising customers about how to get the right message to the right people so real change happens. I'll explore obstacles, attitudes, and challenges that I've faced in hundreds of companies; practical methods for getting your point across; helping others to understand what you are saying; learning to speak their language; and helping them to draw the desired conclusion. This is part art, part science, and maybe a little luck - but I believe there are skills you can learn that will make you a successful communicator and get your message heard.

How to get into ICS security

Mark Heard

This talk is about how to get into ICS security because we don't have enough people! It covers knowing the basics; ICS security standards (like NIST SP800-82 and ISA99/IEC62443), threats to ICS, and basic defense measures.

The Ransomware Threat: Tracking the Digital Footprints

Kevin Bottomley

The continuing evolution of ransomware is a constant threat to businesses of all types. Taking a stroll through the timeline of ransomware from it's infancy to current variants, this session will walk through the methodologies for prevention, containment, and detection both inside the system and by following the digital footprints to hunt it in the wild. TeslaCrypt, CryptoWall and TorrentLocker -- have you or someone you know been affected by ransomware, yet?

InfoSecs in the City - Starting a Successful CitySec Meetup

Panel : Johnny Xmas, Chris Carliss, Fletcher Munson, & Kate Vajda

Founding members of Chicago's (in) famous "BurbSec" meet-ups have assembled a POWERHOUSE panel of influential members of the social InfoSec scene from around the midwest! members from Chicago, Milwaukee and all over Michigan (and maybe more!) will be discussing their various and notably successful "CitySec" frameworks, with the goal of providing you with the knowledge and tools you need to found your own CitySec, or put your existing one on a path to success!

Breaking Through Cellular Gateways and How I Gained Access to One of the US's Largest Energy Companies

Mike Brancato

With cellular networks gaining bandwidth, many organizations are deploying cellular network gateways in remote locations to provide internet and network access. Some of these devices offer no more security than a SOHO router. This presentation will review some of the different types of cellular gateway devices, and identify security concerns. Attendees will learn how to discover these devices, find common configuration problems, identify connected UART devices, and explore potential mitigations.

Ever Present Persistence - Established Footholds Seen in the Wild

Evan Pena and Chris Truncer

Penetration tests do not commonly require testers to establish a long-term presence within a network, but that is not how the real world works. Unless you are facing an insider threat, you have to come to the realization that once attackers get in, they are likely going to install some form of persistence that

will grant nearly (if-not) on-demand access into your network. This talk will document a variety of different persistence techniques that we have seen in the wild, ranging from your dollar store capability to those that are highly engineered. We want you to learn the different techniques we have seen so you can recreate them, or hunt for them in your network.

Forging Your Identity:
Credibility Beyond Words
Tim Roberts and Brent White

Pretending to be an employee is one thing, but owning layers of identities is what has led to owning the data centers, PBX rooms, Security Control Centers and more. If a discerning employee is not buying into your backstory, your credibility can sometimes make or break an assessment. In this presentation, we will discuss document and badge forgery, setting up and forwarding local phone numbers, and fake employee web search results. You will listen to real world scenarios that led to an armed security guard handing over the building keys, facilities opening two-factor authentication restricted areas and more!

IAM Complicated:
Why you need to know about Identity and Access Management
Ron Parker

Do you know where identities are born? How can you tell what an identity can and can't do? What do you do when you realize your refrigerator has an identity of its own? If your IPS blocks your refrigerator you may lose access to your pizza. Identity and Access Management is what connects the identities, accounts, entitlements, roles, permissions, and resources to provide correct access control. All areas of security are dependent on IAM and need to understand how to take advantage of it. This talk will explore the IAM lifecycle showing how to protect it and wreck it along the way.

Put a Sock(et) in it:
Understanding and Attacking Sockets on Android
Jake Valletta

You're probably wondering how someone could possibly fill a 45 minute slot talking about the security implications of sockets (after all, there are only TCP and UDP sockets, right?). In reality, there are several unique types of sockets used by an Android device. These range from network sockets (the ones we are all familiar with), to local sockets, and even kernel-level sockets. When used improperly, these sockets can have devastating effects on the overall security of a device. In this talk, I'll discuss several types of Linux-based sockets found on Android devices and how these sockets have historically been used to compromise devices. I'll also provide the tools and techniques necessary to enumerate and interact with these sockets on your own device.

At the Mountains of Malware

Wes Widner

A "how to" on setting up a malware pipeline of your own. This talk includes pointers on obtaining a steady stream of malware, extracting features from malware, and finally how to go about generating actionable threat intelligence from that malware. This talk will include hands-on demonstrations of each component of the malware pipeline

Collection and Detection with Flow Data : A Follow Up

Jason Smith

Last year I gave an introduction on what exactly flow data is, what it looks like, and a basic rundown on how to get started with it. Since then I've received a *lot* of requests that I expand on the questions of "how to get started" as well as "and then what"? This year I'll be giving a very brief recap on what flows are and why you should collect them, and I'll be spending most of my time on the question of how to set up free tools to provide enterprise flow monitoring for security and situational awareness. I'll also be spending significant time answering "and then what?" with real-world practical examples that I've prepared as well as live examples from questions in the audience.

Container Chaos: Docker Security Container Auditing

Chris Huntington

Docker is one of the hottest tech trends of the past few years. Containerized applications are convenient, scalable, and when implemented correctly can offer some security advantages. However, with nearly 30% of Docker containers showing that they are vulnerable to threats, how can the security team deal with this powerful new DevOps tool? In this talk, we will explain some of the issues with securing Docker from privilege issues with the daemon to improper container builds. We will then discuss best practices for deploying Docker securely without losing scalability.

It's Not If But When: How to Create Your Cyber Incident Response Plan

Lucie Hayward and Marc Brawner

A strong incident response plan is a key component of any organization's cyber defense. Many organizations, however, have an ineffective, or no cyber response plan in place at all. We only need to look to the daily news to see the impact that an ineffective cyber response can have on an organization's bottom-line. A solid plan can help you identify and respond quickly to a cyber incident, and mitigate the financial and reputational costs.

Threat Modeling the Minecraft Way

Jarred White

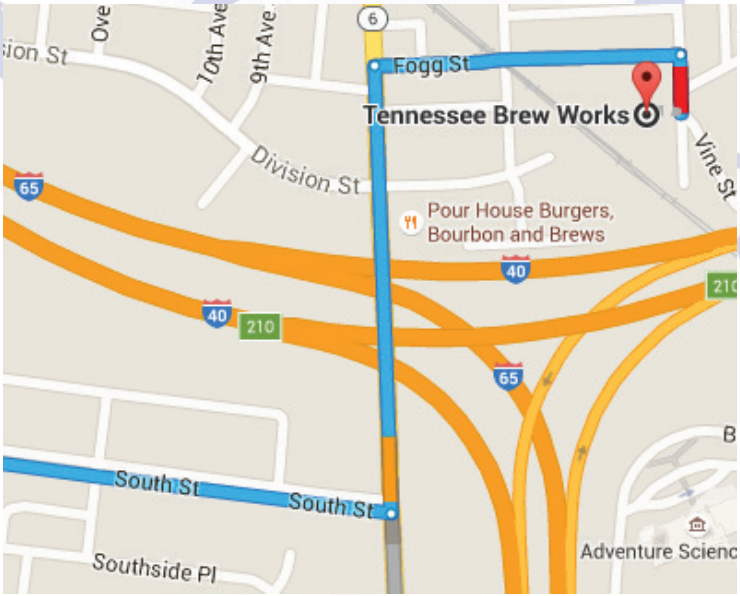
Your 10 year old is better at threat modeling than you! No, really. The secret is the addictive phenomenon known as Minecraft, which teaches kids to solve puzzles and secure their environments in three-dimensional space. Like you, they have to protect their loot and survive in a world filled with perils and bad guys actively out to get them. I'll share stories about the myriad ways I've died in Minecraft, and how those experiences have made me better at designing systems which protect against the real-world equivalent of zombies, spiders, and creepers.

BSIDES NASHVILLE PARTY

Sponsored by:

QUALYS®
CONTINUOUS SECURITY

Head North on Granny White Pike
Continue to 12th Ave South
Right at South St
Left at 8th Ave South
Right at Fogg St
Right at Ewing Ave



Tennessee Brew Works
809 Ewing Ave,
Nashville, TN 37203
www.tnbrew.com

SPONSORS

LIPSCOMB UNIVERSITY
COLLEGE OF COMPUTING & TECHNOLOGY
PLATINUM SPONSOR

QUALYS® CONTINUOUS SECURITY
GOLD SPONSOR

PARTY SPONSOR

netWorks
SILVER SPONSOR

SOPHOS
SILVER SPONSOR

SOLUTIONARY
AN NTT GROUP SECURITY COMPANY
BRONZE SPONSOR

ISSA
Information Systems Security Association
Middle Tennessee Chapter
BRONZE SPONSOR

TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE
BRONZE SPONSOR

AppSec CONSULTING
Security Compliance & Assurance
FRIENDS of BSIDES

IBM Security
Intelligence. Integration. Expertise.
FRIENDS of BSIDES

no starch press
FRIENDS of BSIDES

VACO
Free Yourself.
FRIENDS of BSIDES

Magenta Monkey Studio
GRAPHIC DESIGN

We would again like to thank our sponsors, volunteers and attendees.

Without everyone's generosity and time we would not be able to put on this awesome security conference.

We could not have done this event without you!

BSIDES NASHVILLE