PROGRAM
2015

BSIDES NASHVILLE

WWW.BSIDESNASH.ORG
@BSIDESNASH

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

BSides Nashville 2015

Welcome

On behalf of the Organizing Committee, volunteers, speakers and sponsors we are pleased you are here.

It's never easy to assemble a conference. After the success of BSides Nashville in 2014, we had to do it again: just like hot chicken and good beverages, the thrill of bringing forth a good conference is addicting.
To our sponsors: Thank You from the bottom of our hearts. We could not do this without your support. Each of you bring resources and enthusiasm to the event, and we offer a special "thank you" to Lipscomb's College of Computing and Technology for providing the perfect space and atmosphere. We are all students of the security craft, so being "schooled" by our speakers and taking a swim in the Phish Bowl is a good thing….

We want BSides Nashville to be more than talks and swag. We intentionally avoided tight schedules in the planning want all of you 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 sit a spell. Around here, make friends around the tables while fixin' to pick locks or mess with a Raspberry Pi. (Not certain what "fixin' to" means? That's okay because we're not too sure either. Doesn't matter….)

Of course, our speakers have brought "the good stuff" again in 2015. We spent weeks going over the talk proposals, and it was a joy to see all the talent who wanted to be a part of our little con. 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. Come play in the SCADA sandbox, spin a tumbler at the lock-pick roundtable, or see what the Nashville Makers are doing. Come see, meet, talk… and leave inspired.

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

Lauren Rogers - President

Lauren is a corgi loving, bourbon connoisseur who supports her coffee addiction by managing an InfoSec team. She has spent her career supporting and securing the IT infrastructure for a variety of organizations including the DoD and CMS contractors. When not working she is studying various attack vectors or being dragged outside to enjoy the Tennessee sunshine. Lauren is skilled at reading, interpreting and translating FISMA requirements into plain English, but no worries she is seeking treatment.

Geoff Collins - Treasurer

Geoff Collins @digiears is Belmont University alum, a Project Manager and Support Tech for Net Works, LLC. Proud husband and father of three children, he always has pictures ready on his phone for you to see. He has lived in Nashville for 23 years, just long enough to have picked up a twang. He has been an audio engineer, pool boy, barista, projectionist and librarian before embracing his calling. A lifelong nerd, he finally has a career to show for it and is very proud to be a founding member of the BSides Nashville committee.

Finn Breland - Secretary

Finn Breland graduated from Lipscomb University in 2008 and has enjoyed working with college students ever since. From 2008-2011, he served as an English teacher in Shiyan, China. After returning to the US, Finn advised high school students on their college choices as an educational consultant before returning to his alma mater. At the College of Computing and Technology, Breland works with technology students to connect them to opportunities in the technology industry. He is passionate about the growing IT community in Nashville and spends much of his time helping to build that community.

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

Gabriel Bassett..... Badge® Wrangler
Tommy Wolosin.....Swagger Supplier
Michael St Vincent.....Minion
Adrian Crenshaw.....Norse god & AV
Scott Haber.....Silent Partner
Nathan Croy.....Phish Monger
RC.....The Force
Shelby Grey.....One-Shade
Jennifer Samardak.....Nerf Herder

Partner with Nashville's pacesetter in technology education.

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

Information Security

Information Technology Management

Informatics and Analytics

Software Engineering

LBMC

Security & Risk Services

www.lbmcsecurity.com

KEYNOTE SPEAKER:

Trey Ford
@TreyFord

Trey Ford is the Global Security Strategist at Rapid7 where he serves as a customer resource, industry and community advocate. Over the last 15 years, Trey ran Black Hat events worldwide as General Manager, and served functions ranging from incident response, product management, PCI QSA and security engineer for a variety for industry leaders including Zynga, McAfee, FishNet Security and WhiteHat Security.

Slade Griffin
@Slad3g & @Cyphoss

Slade Griffin is the owner of Cyphoss Security where he leads the cyber security services practice. He has over 15 years experience in cyber security specializing in vulnerability assessments, penetration testing, risk assessment, security program development, forensic analysis, and incident response. Slade is passionate about security; blending his experience in the public, private and military sectors to help others tackle their own cyber security challenges. Prior to founding Cyphoss Security, Slade worked in multiple roles within the information security field ranging from forensic analysis, incident handling, policy development, vulnerability assessments, and penetration testing. He also served in the United States Navy for six years in roles related to information systems, communications, and physical security. Slade is a speaker and instructor on the topic of emerging threat and attack vectors in multiple forums including conferences, training courses, and universities both as lecturer and instructor.

Ron Parker
@scmunk

Ron Parkeris the Senior Enterprise Security Architect for Unum, the leading group and individual disability insurance provider. Ron has decades of experience successfully designing and developing secure application and nfrastructure 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. Ron is also a non-reluctant CISSP.

Chris Rimondi
@crimondi

Chris Rimondi is the Application Operations Manager at FireEye's Cloud Analytics Engineering business unit.

Stephen Haywood

@averagesecguy

Stephen Haywood is a developer, security tester, author, blogger, and all around nice guy. You can read his blog at averagesecurityguy.info, and you can read his book "Hack Yourself First" at https://averagesecurityguy.files.wordpress.com/2015/01/hack-yourself-first-final.pdf

Chris Scott

@Cyb3r_Assassin

In 2000, Chris released his first commercial app, "Advanced Timer", which was the most widely adopted time candle chart utility in the commodities day trading practice in the early 2000's. Chris also developed the first Instant Messaging proxy platform for the AIM protocol in 2001. These applications were designed as early remote social engineering tools functioning as communication drop bots and incognito mail platforms. In 2007, Chris was an early adopter of smart phone development where he built custom ROM's for the windows PPC platform. More recently, Chris has spent time working in cryptography with the goal of ensuring the protection of sensitive information no matter where it travels, and focusing on internal IT architectural and administration vulnerabilities. Chris's passion for network intrusion and coding expertise led him to develop a comprehensive framework for wireless network intrusion, N4P, which is featured in the repository of Pentoo Linux. In addition to his technical expertise, Chris is a noted writer, and was recognized as a finalist for best new security blogger by the Security Bloggers Council at the 2014 RSA Security conference. Chris has also enjoyed speaking at national security events.
Prior to his career in InfoSec, Chris spent 11 years at a national level and 8 as professional competitor in Motocross before retiring as a competitor to focus on his InfoSec career. He still serves as a mentor and trainer in the motocross community.

Tim Roberts and Brent White
@ZanshinH4x & @Brentwdesign

Tim and Brent are currently Offensive Security Consultants within Solutionary, and have recently spoken at Def Con 22 and the ISSA International conferences. Their 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 and management roles across multiple industries including healthcare and government. He has conducted highly successful Red Team Assessments.

Brent has held the role of Web/Project Manager and IT Security Director at the headquarters of a global franchise company. His specialty is in application, Social Engineering and Wireless Assessments.

Michael St. Vincent
@JustOnePing

Michael St. Vincent is an InfoSec professional with over two decades of security and risk management experience. His work includes developing, implementing, and leading security programs in financial, defense industry, and ISP organizations. Along with Bsides Nashville, he currently serves the Metro Nashville Mayor's Information Security Advisory Board, the Middle Tennessee Chapter of ISSA, and the Nashville-based TN CISO Roundtable. During downtime, he supports youth development programs in local, national, and international activities.

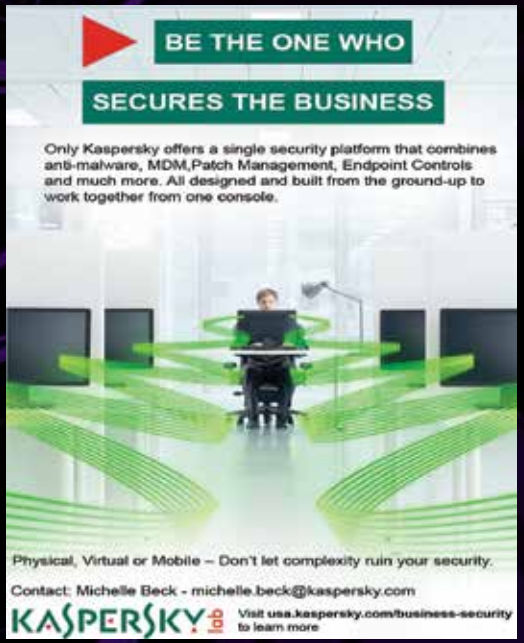
Ben Miller
@Securithid

Information systems specialist turned offensive security expert, Ben Miller brings a unique mix of networking, compliance and security experience to the table. As a Certified Ethical Hacker for Parameter Security, Miller identifies and exploits weaknesses in clients' networks – emulating a real-world attack.

Prior to Parameter Security, Ben was employed by Lincoln County Medical Center where he gained extensive knowledge of meeting and maintaining HIPAA compliance regulations on an ongoing basis, creating and deploying as well as securing systems against malicious hackers.

Joshua Tower
&
Russell Butturini
@tcstoolHax0r

Joshua Tower is the newest Information Security Engineer on Russell's team. Fresh out of graduate school, he is often found searching for vulnerabilities on web apps and (sometimes) breaking servers. With his developer background, Joshua is always thinking of new ways to automate the five-hundred pound gorilla known as compliance so that he can get back to improving his technical abilities.



Russell Butturini is the Senior Enterprise Security Architect at a large wellness solutions company in Nashville, where he oversees everything security that isn't compliance (which bores him to tears). He has presented at several conferences such as DEFCON and Derbycon, and authored multiple security tools, such as the U3 incident Response Switchblade, The Network Attached Storage Enumerator, and NoSQLMap. These are amazing accomplishments considering he was once fired from a job at Wendy's after a week and a half of employment.

Heather Pilkington

Heather Pilkington is a penetration testing consultant for Accuvant, and formerly a member of Spiderlabs. She has inflicted her fast-paced and humor driven speaking style on audiences at local conferences and bsides events for several years. With more than ten years of experience in information security (including more than 5 years in threat and vulnerability management), she has a breadth of disciplines from which to draw.

NSAKEY
@_NSAKEY

I'm just a guy who likes to keep up with infosec news and dabble in related things as a hobby.

Johnny Xmas

@J0hnnyXm4s

@J0hnnyXm4s is the Boss of Level 3 of The Internet. He has a +16 to save vs. Horse-Limes, and his weaknesses include sloths and funny porn. He's been independently awesome since late 2002, and professionally awesome for the past 3 years. While not (ever) busy touring as the world's most famous professional speaker, he definitely, absolutely does NOT pass the time by posing as a scantily-clad Thomas Jefferson at the mall on 83rd and Wellington. That was definitely someone else, and further allegations of this nature will result in swift legal action against you.

Jason Smith

@automayt

Jason Smith is an intrusion detection analyst by day and junkyard engineer by night. Originally from Bowling Green, Kentucky, Jason started his career mining large data sets and performing finite element analysis as a budding physicist. By dumb luck, his love for data mining led him to information security and network security monitoring where he took up a fascination with data manipulation and automation. Jason is the co-author of Applied Network Security Monitoring, creator of FlowPlotter, and co-developer of FlowBAT.

Jason has a long history of assisting state and federal agencies with hardening their defensive perimeters and currently works as a Security Engineer with Mandiant. As part of his development work, he has created several open source projects, many of which have become "best-practice" tools for the DISA CNDSP program.

Chris B. Simmons

Chris B. Simmons is an Assistant Professor in the College of Computing and Technology at Lipscomb University. His research involves enhancing secure software development standards and the development of knowledge management systems for secure software and cyber-attack response.

Vivek Shandilya

Vivek Shandilya is an adjunct faculty member at Lemoyne Owen College, Memphis. He has defended his PhD in the Department of Computer Science at University of Memphis, Memphis, TN. He has a BE in Electronics and Communication Engineering from Bangalore University, India and a MS in Computer Science from University of Memphis. His research interests involve establishing the structures in the interaction of intelligent agents with conflicting and mutually unknown motivations, in dynamic stochastic systems. This problem manifests in optimization and security situations of the computational systems as well as in the broad socio-economic systems. The work involves Information theory, mathematical modeling and design and analyses of algorithms for learning and optimization. His current work involves applying game theory to cyber security.

BSIDES NASHVILLE

Magenta Monkey Studio
MARYMCONLEY.COM

Tim Fowler
@roobixx

Tim Fowler is a security consultant with the Western North Carolina security firm mountainsec LLC. He frequently speaks throughout the Southeast on various topics ranging from information security, open source in the enterprise and emerging open source technologies. Formally an IT Administrator for a large automotive manufacturer and an open source network appliance developer, Tim has spent years developing an understanding of the weaknesses and issues that we as an industry are currently dealing with in our IT departments today. Over the last 7 years, he has devoted a lot of time to specifically researching, testing and creating education and awareness programs around wireless (in)security and the issues that plague 802.11 as well as developing open source solutions.

Together is Better.

ACCUVANT fishnet SECURITY

General Inquiries
(800) 574-0896
info@accuvant.com

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.

© 2015 Qualys, Inc. All rights reserved.

Red.....102
Green....110
Blue.....100
Purple...108

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: Trey Ford		
10:15 - 10:30	**Coffee Break**		
Time	**Green**	**Red**	**Blue**
10:30 - 11:30	Name: Heather Pilkington Talk: So you want to be a pentester?	Name: Tim Roberts & Brent White Talk: From Parking Lot to Server Room	Name: Jason A. Smith Talk: Applied Detection and Analysis Using Flow Data
11:40 - 12:40	Name: Tim Fowler Talk: We Built This & So Can You! "Why does open source matter?"	Name: Chris Scott Talk: N4P Wireless Pentesting So Easy Evena Cave Man Can Do It!	Name: Chris Rimondi Talk: Using devops monitoring tools to increase security visibility
13:00 - 14:00	**LUNCH sponsored by**		
14:00 - 15:00	Name: Johnny Xmas Talk: That's NOT my RJ45 Jack!: IRL Networking for Humans.	Name: _NSAKEY Talk: hashcat	Name: Ben Miller Talk: The Great Trojan Demo
15:10 - 16:10	Name: Stephen Haywood Talk: Finding Low Hanging Fruit with Kali.	Name: Chris B. Simmons & Vivek Shandilya Talk: Use of Attack Graphs in Security Systems	Name: Michael St. Vincent Talk: Nobody Understands Me: Better Executive Metrics
16:20 - 17:20	Name: Slade Griffin Talk: What do infosec practitioners actually do?	Name: Russell Butturini & Joshua Tower Talk: Skiddiemonkeys: Fling "stuff" at your Defenses and See What Sticks	Name: Ron Parker Talk: Agile and Security Oil and Water?
17:30 - 17:40	**Closing Ceremonies Sponsored**		
18:00 and Beyond	**After Party at Belcourt Taps**		

Presentations

KEYNOTE SPEAKER:

Pondering the False Economy of Secrets

Trey Ford @TreyFord

Risk management, troubleshooting, and post mortem analysis became very different terminology when trading a CISSP study guide for the "Pilot's Handbook of Aeronautical Knowledge" (You *do* know how to spot the Pilot or Ph.D. in a room… right?)
I've spent years pondering how the checklists, "deadly attitudes", preflight planning, course correction, and a run-in with the "Flight Standards District Office" might profit our industry, where feedback is not always as immediate or obvious. In this hour, I hope to share some of my failures-explore some lessons learned, and ask hard questions. I'd like to reconsider the false economy of secrets we live in- and the actions that support our adversaries.

What do infosec practitioners actually do?

Slade Griffin @Slad3g & @Cyphoss

Quite a few people often think that working in this field is "cool" and "fun." While it can be, it does present some interesting challenges especially to bright and talented people. This talk will be a discussion about the perception of what the students think is involved in the field compared and contrasted with the speaker's 15 years of experience working for too many companies before finding where he belonged. The goal is to set adequate expectations for people interested in this field and to allow for Q&A with an experienced practitioner that wants quality people to be working in this field.

Agile and Security - Oil and Water?

Ron Parker @scmunk

How do we make our security tips, techniques and tools be enablers in our agile development surroundings?
Part of the problem is scale. You and your other security professional friends can't always be totally engaged with each and every delivery team. There will always be more people making security and risk decisions than there are security consultants. Another key is getting out of the way. You need to enable people to make the risk decisions on their own schedule. They can't wait to attend yet another meeting or spend gargantuan efforts on security work that may or may not be needed.
We need to build a security environment that that fosters good practices and at the same time fits well into more modern and agile methodologies.
There are ways to design security tasks so they can be embedded into just about any methodology. This talk will walk through implementing a Security Development Lifecycle using the OWASP Software Assurance Maturity Model as a guide. Quick and Easy Security should not be an oxymoron.

Applied Detection and Analysis Using Flow Data

Jason A. Smith @automayt

While network flow data isn't a new concept, it is easily one of the most powerful data types you can have in your arsenal as a network defender. It is incredibly low overhead, easy to setup and maintain, and provides tremendously flexible capabilities for network security monitoring (NSM) detection and analysis. In this presentation, we will take a look at flow data from the perspective of the NSM analyst. To begin, we will harness the power of statistics to demonstrate how flow data can be used for detecting both structured and unstructured threats using techniques that go beyond simple signature matching. Next, I will discuss the concept of friendly intelligence and how flow data can be used to profile devices on your network so you can understand what normal communication looks like. Finally, I will describe how flow data can be used to augment the analysis of network security events that are detected by other mechanisms. During this presentation, I will also demonstrate FlowPlotter, an open source tool I've developed to aide in visualizing flow data for detection and analysis. I'll also introduce and demonstrate FlowBAT, a graphical flow-based analysis tool that Chris Sanders and I developed to break the significant barrier of entry into Flow Analysis. Every concept I discuss in this presentation will be demonstrated with practical, real-world scenarios complete with real data using the SiLK toolset. You will leave this talk with techniques you can apply to your network immediately with incredibly low overhead and high impact, and scripts to get everything running in minutes.

Finding Low Hanging Fruit with Kali

Stephen Haywood @averagesecguy

Every network has low hanging fruit, easy to find and fix vulnerabilities that will quickly improve its security posture. In this presentation we will discuss how to use Kali Linux to find the low hanging fruit on your network. We will focus on finding unnecessary services, weak passwords, exploitable vulnerabilities, and unencrypted services.

From Parking Lot to Server Room.

Tim Roberts & Brent White
@ZanshinH4x
@Brentwdesign

In this presentation we will be covering methods of exploiting the human element of security and how to continue the manipulation during social engineering and Red Team engagements. We will be sharing stories and experiences that illustrate the subject and focuses on starting with covert parking lot reconnaissance and peeling away security until the tester reaches the server room. Abstract: Pretending to be an employee is one thing, but owning layers of identities is what leads to owning the data center. In this presentation you will listen to real world scenarios that led to armed guards opening biometric access controlled server rooms for the hacker to secretaries handing over an executive's laptop. All of this and more, from parking lot to pwnage.

hashcat

_NSAKEY @_NSAKEY

AAfter briefly touching on the general concept of password cracking, the focus of the talk will be on the effectiveness of different attack modes in hashcat, with a heavy emphasis on rule-based attacks. While the name of the talk is "hashcat," this talk will almost exclusively discuss the GPU-enabled versions (Specifically cudahashcat). The final phase of the talk will include the results of my own experiments in creating rule sets for password cracking, along with an analysis of the known plaintext passwords from the test hash list.

Nobody Understands Me: Better Executive Metrics

Michael St. Vincent
@justoneping

As a maturing field, information security has a growing number of strong technical practitioners with a very small number successfully transitioning to speaking relevantly with executives on security as part of the overall business strategy. Just as strong CIOs have moved from talking in processors and routers, leaders in information security are bridging discussions of business risk and competitive landscapes with understandable metrics. During this session, some model metrics will be discussed taking typical "geek numbers" into CxO presentations by appropriate transformation and interpretation. Participations will be invited and challenged to raise questions for additional executive metric models.

Using devops monitoring tools to increase security visibility

Chris Rimondi @crimondi

Getting visibility into important security events in your network can be difficult and expensive. This presentation focuses on using popular devops tools to gain insight quickly and cheaply. Use cases will be covered with tools such as Graphite, Statsd, Seyren, Grafana and Logster.

Wireless Pentesting with N4P: So Easy Even a Cave Man Can Do It

Chris Scott @Cyb3r_Assassin

Chris will discuss wireless penetration testing using the network management suite he has written called n4p. N4p takes the pain away from system network device management during wireless pentests (WPA2 WPS) and the lengthy command memorization while bringing the ease of a framework based design for efficient offensive tasks. N4p also brings you the only solution for more incognito minded individuals by controlling your VPN and device bridges on the fly. By doing this we provide your MITM attacks with a strong attack base you could take nearly anywhere from SSLstrip to pulling off elaborate phishing with SET and redirection in iptables. N4p provides you with a well planned out comprehensive iptables base script that provides adapter and port limitations out of the box for your rogue AP. You could restrict your victim's activity onto specific ports for easy of monitor/sniffing and be alerted real time with the ip of any new victims connecting.

TrustedSec
INFORMATION SECURITY MADE SIMPLE

netWorks
networks that work™
SOPHOS

Skiddiemonkeys: Fling "stuff" at your Defenses and See What Sticks

Russell Butturini & Joshua Tower
@tcstoolHax0r

Every security team invests tons of money in detective and preventative technologies. But how do they know they are working? Sure, there are pen tests, vulnerability scans and the old ""if we see stuff happening it's probably OK"" theory, but none of these reflect real world attacks. Security teams need QA tools for their defenses designed to simulate targeted attacks by attackers of various intelligence levels in a distributed fashion. This helps teams to understand what their tools are seeing and, more importantly, what they are not seeing. This talk will examine these gaps, and also demo a tool, Skiddiemonkeys. This tool is based on the Netflix ""Chaos Monkey"" principles and designed to create a variety of randomized, semi-controlled bad actors across a distributed environment to test security tools and help security teams learn how they react to or reflect malicious events on the network.

So you want to be a pentester?

Heather Pilkington

Fairly or unfairly, penetration testing has attracted a lot of interest from infosec wannabes. As a result, there seem to be a lot of presentations catering to aspiring penetration testers that turn out to be a 50 minute sign that says "Learn Metasploit." This presentation is a fast-paced, often hilarious, 30-45 minute (tailorable for room for questions) romp that explores practical career points from a penetration tester. Rather than a dictionary of tools you should learn, or an encyclopedia of certifications, this presentation explores the breadth of infosec as a career discipline, the varieties of pentesting within that, and day today challenges within pentesting consulting and corporate security as a result of surveying dozens of pentest pros. The presentation will explore traits of successful pentesters who attack these daily challenges and offer insight into penetration testing as a career for those who think they may be interested.

The Great Trojan Demo

Ben Miller @Securithid

Have you ever seen a Trojan demonstrated before you live? Was it from one vm to another? Probably! It shows the frightening capability but leaves you wondering: is that really all there is to it? Hacker Ben Miller was asked, "Why doesn't anyone do Trojan demos of how they work over the Internet?" The first reason Ben could provide was, "It's Hard!" However, that's not a reason NOT do it. In this talk, Ben Miller demonstrates his tiered test network, the Trojan communication receiving setup, and demonstrates (ON LIVE VIDEO) how the communications work and are easy to hide.
This talk is focused on teaching the new hacker steps to test their ideas. Additionally, this talk is informative to the defensive side of the table for how to detect and thwart certain Trojan and covert communication behaviors."
Information systems specialist turned offensive security expert, Ben Miller brings a unique mix of networking, compliance and security experience to the table. As a Certified

Ethical Hacker for Parameter Security, Miller identifies and exploits weaknesses in clients' networks – emulating a real-world attack.
Prior to Parameter Security, Ben was employed by Lincoln County Medical Center where he gained extensive knowledge of meeting and maintaining HIPAA compliance regulations on an ongoing basis, creating and deploying as well as securing systems against malicious hackers.

Use of Attack Graphs in Security Systems

Chris B. Simmons & Vivek Shandilya

Attack graphs have been used to model the vulnerabilities of the systems and the their potential exploits. The successful exploits leading to the partial/total failure of the systems are subject of keen security interest. Considerable effort has been expended in exhaustive modeling, analyses, detection and mitigation of attacks. One prominent methodology involves constructing attack graphs of the pertinent system for analysis and response strategies. This talk will present a survey of the current state of technologies in attack graph generation and use in security system. Based on our research, we identify the potential, challenges and direction of the current research in using attack graphs.

That's NOT my RJ45 Jack!: IRL Networking for Humans

Johnny Xmas @J0hnnyXm4s

Following close on the heels of last year's incredibly successful "Attack Paths: How to Get a Job in Infosec" talk, this instructional session discusses the specifics behind building up the soft skills necessary to effectively socialize and network with other human beings. This seminar will go beyond the obvious "do this; don't do that" information and focus heavily on how, where and what to practice in order to refine your skills. While most of the information will apply to all social situations, this seminar will have a career focus (not just InfoSec!), helping to provide information for not only job interviews, but also for professional networking to get those interviews in the first place. Guaranteed to be something in here for everyone, from the Basement Nerd to the Social Engineering Expert.

We Built This & So Can You! "Why does open source matter?"

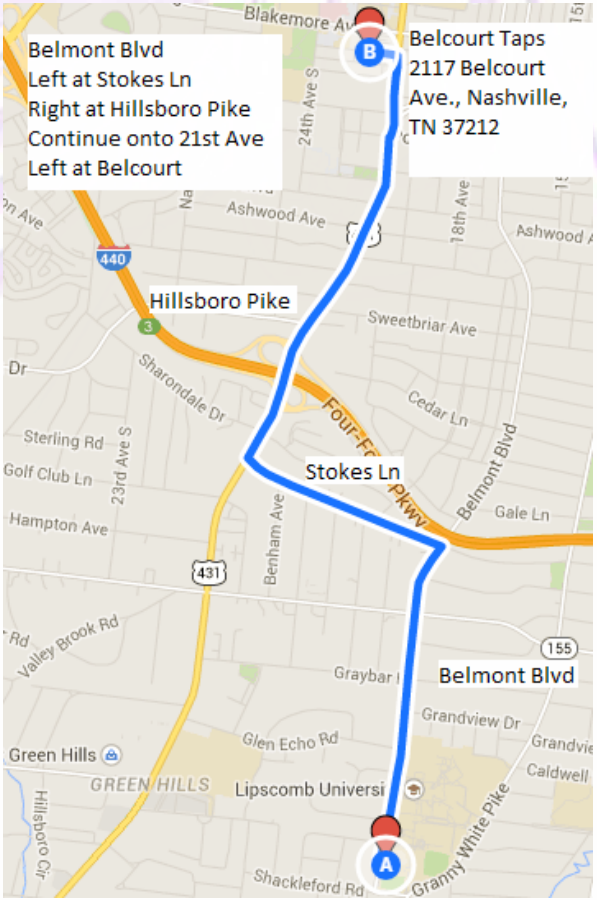
Tim Fowler @roobixx

The information security industry has been built on open source. We rely on it more than almost any industry out there and we leverage it to do amazing things and so can you!
But why does open source matter?
In this talk we will look at why open source is so important to the InfoSec world as well as diving into some of the tools and processes that you can leverage as you get started.

Party

Belcourt Taps
2117 Belcourt Ave.
Nashville, TN 37212

belcourttaps.com



Sponsored by:

QUALYS
CONTINUOUS SECURITY

Parameter

SPONSORS

LBMC Security & Risk Services
PLATINUM SPONSOR

LIPSCOMB UNIVERSITY College of Computing & Technology
PLATINUM SPONSOR

QUALYS
GOLD SPONSOR PARTY SPONSOR

Parameter
PARTY SPONSOR

netWorks
SILVER SPONSOR

SOPHOS
SILVER SPONSOR

TrustedSec
SILVER SPONSOR

KASPERSKY lab
SILVER SPONSOR

ACCUVANT fishnet SECURITY
SILVER SPONSOR

Sword & Shield Enterprise Security
BRONZE SPONSOR

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

© B-Sides Nashville 2015