@BsidesNash

PROGRAM
2014

bsidesnash.org

Welcome

On behalf of the organizing committee, we would like to welcome all of you to the inaugural Bsides Nashville event. It gives us great pleasure to see each and every one of you offer one of your precious Saturdays to gather here, at Lipscomb University's campus, to learn from our fantastic presenters, to share your stories with others, to greet old friends and to meet new ones.
To our sponsors, our partners, we could not have done this without you. Your financial support is what makes this possible. You truly represent the best of the industry.

To the presenters who, being true leaders of the community made the trip to Nashville at their own expense from different places around this great country of ours, we thank you! Thank you for sharing your experience, your knowledge, with all of us.

To all of you who are thirsty for knowledge and continue learning and growing professionally, we thank you.
We welcome you and thank you for making our vision come true.
Have a great time, learn a lot, and make great friends.
If you see us walking around, stop us, say hi. We want to meet all of you!

Bsides Nashville Organizers

Adrien Crenshaw

Geoff Collins

Lauren Rogers

Breland Finn

Gabriel Bassett

Ed Rojas

Organizers

Ed Rojas

Network Architect with more than 27 years experience in the LAN/WAN industry. Edgar has extensive international experience, leading groups of engineers and developing new markets in USA, Europe and Latin America. Founder of Security Zone, one of Latin America's premier infosec events during the two years he organized it. Now proud to be organizing Bsides Nashville together with the other fantastic organizers

Gabriel Bassett

An explorer of ideas. With a background in weapon system information security, Gabriel spends his days architecting security in healthcare and his nights studying data analytics. Gabriel has developed patent pending technology for using machine learning to profile networks using netflow as well as for using Bayesian probability and economic cost to model an organization's security posture using an attribute-influenced attack graph.

Adrian Crenshaw

Adrian Crenshaw has worked in the IT industry for the last seventeen years. He holds a Master of Science in Security Informatics, works for TrustedSec as a Senior Security Consultant and is one of the co-founders of Derbycon.

Geoff Collins

Lauren Rogers

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.

Breland Finn

Master of Science in Information Security (InfoSec)

The existing shortage of skilled workers and anticipated growth in the IT field creates the demand for individuals with the knowledge and skills necessary to oversee and secure organizations' data and information in an ethical manner. Today, companies are in desperate need of information security experts. It is critical that organizations lock down their information and continually look for new ways to keep it secure to new threats.

Lipscomb University offers a Master of Science in Information Security degree designed to develop leaders ready to meet these challenges. This degree—which focuses on both the managerial and design issues in information security—will prepare you for a career in a variety of scenarios from large corporations to the development of your own entrepreneurial information security capability.

- Ideal student has a degree in IT or is currently working as an information technology professional
- Faculty are leaders in their field, dedicated to working with students and offering personalized attention not often found at other institutions
- Weekend classes are held each month, with 36-hour coursework delivered in as little as 12 months plus two months of individual capstone project work
- "Cohort" program model, which means you stay with the same students through the entire program learning from, supporting and networking with each other
- Prepares students for leadership technology positions with above-average compensation

Today, companies are in desperate need of information security experts. Earn a master's degree from Lipscomb University and earn the credentials you need to be a leader in this exciting and growing field.

LBMC

Security & Risk Services

www.lbmcsecurity.com

KEYNOTE SPEAKER: JACK DANIEL

(@jack_daniel)

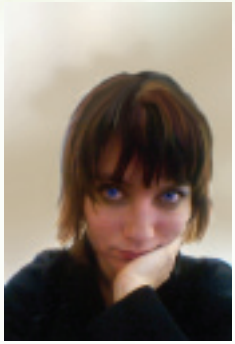
Photo by : A. Jolly (@Jolly)

It is a great pleasure to announce our confirmed keynote speaker is Jack Daniel. Information Security Curmudgeon, Security BSides Co-Founder, Increasingly Reluctant CISSP, MS MVP for Enterprise Security, Technical Product Manager at Tenable Network Security, Co-host at Pauldotcom podcast.

Contact: jdaniel@voodooelectronics.com

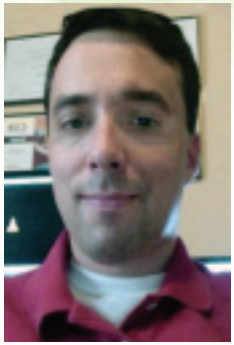
Eve Adams

(@HackerHuntress)



Senior Talent Acquisition Expert

Eve Adams is Senior Talent Acquisition Expert at Halock Security Labs, a full-service information security advisory in Schaumburg, IL. Eve leverages three years of security staffing experience to drive recruitment for both internal Halock roles and client placement. She also spearheads Halock's social media presence and counts Twitter as one of her most powerful recruiting tools. She's passionate about information security, thinks most recruiters are doing it wrong, and naively believes technology can change the world for the better. In past lives, she has been a writer, translator and reptile specialist, among other things. While she is officially OS-agnostic, she runs Ubuntu 12.04 at home.



Russell Butturini

(@tcstoolHax0r)

Russell Butturini is the Senior Enterprise Security Architect at Healthways, where he is responsible for application security and penetration testing for the enterprise. Russell has created multiple open source penetration testing and incident response tools such as NoSQLMap, Nasnum, and the U3 incident response switchblade. Also, Russell is a regular guest on information security podcasts, having appeared on Hak5, Securabit, and the Tenable Network Security podcast. In 2013, Russell founded the NoSQLMap project, an automated tool for testing NoSQL databases and web applications, which he current leads and co-develops with Maurizio Abbà. His new goal in life is to teach his 5 year old Python before she leaves Kindergarten.

Paul Coggin
(@PaulCoggin)

Paul Coggin is an Internetwork Consulting Solutions Architect with Dynetics, Inc in Huntsville, Alabama. Paul is responsible for architecting and securing large complex tactical, critical infrastructure and service provider networks. Paul's expertise includes tactical, service provider and ICS\SCADA network infrastructure hacker attacks and defenses as well as large complex network design and implementation. Paul's experience includes leading network architecture reviews, vulnerability analysis and penetration testing engagements for critical infrastructure networks.
Paul is a frequent speaker on cyber security offense and defense issues related to service provider and critical infrastructure. He has presented at conferences around the world including DeepIntel, DerbyCon, BSides, Hacker Halted, COUNTERMEASURE, TakeDownCon, DeepSec, SCADA [in]Security and the DoD Cyber Crime Conference. Paul is a Cisco Systems Certified Instructor # 32230, Certified EC-Council Instructor and a certified SCADA security architect. He has a BS in Mathematics, an MS in Computer Information Systems and is currently pursuing an MS in Information Assurance and Security. In addition he holds a wide array of certifications from Cisco, EC Council, ISC^2 and others.

Adam Len Compton
(@tatanus)

Adam has been a developer, researcher, and professional pentester. Adam has over a decade and a half of experience in network security, incident response, security assessments, and penetration testing. Adam has over 2 decades of programming experience. Throughout Adam's career he has worked in various aspects of information security for both the government and private sector. Adam is a co-founder of www.seedsofepiphany.com and the creator/maintainer of www.ExploitSearch.net

Lucas Gates

(@lucasgates)

Manager at Risk Services at LBMC Security & Risk Services. Lucas has lead development and engineering teams to enhance security solutions for a Fortune 200 company; spearheaded corporate hardening project that led to over 30% reduction in penetration test findings. He has architected and overseen development of an information security portal for a health care company, ensuring alignment with IT Security Compliance objectives and requirements. His work with designing software licensing management application has contributed to a seven figure reduction in licensing cost. Lucas has also empowered compliance engineers in solution development and implementation projects.

Previously, Lucas has managed web solution development for security product provider and Internet marketing subsidiary, ensuring alignment with business objectives and requirements. Lucas also enjoyed providing ongoing web site, network, and system / application maintenance, including enhancements, bug fixes, and security implementation.

When Lucas first arrived in the United States, he served in an IT support capacity for globally distributed scientists and system administrators, with a focus on Linux and IRIX support, providing multilingual issue response and resolution in English, Portuguese, and Spanish.

Lucas has enjoyed teaching co-workers and others Python development skills as well as penetration testing techniques. He also devotes time to hacking challenges and hacking competitions. A native of Belo Horizonte, Brazil, Lucas currently lives with his wife and daughter in Nashville.

Salvador Grec

(@grecs)

Grecs has over 17 years experience, undergraduate and graduate engineering degrees, and a really well known security certification. Despite his formal training, grecs has always been more of a CS person at heart going back to his VIC-20, Commodore 64, and high school computer club days. After doing the IT grind for five years, he discovered his love of infosec and has been pursuing this career since. Currently, he spends his days doing cybersecurity paperwork drills in building multi-billion dollar government systems. At night he runs a local infosec website and tries to get some hands-on skillz.

Adam John
(@ajohn76)

Adam John is a security practitioner that has over a decade of experience in healthcare security and IT operations. He has worked in one of the top research hospitals in the United States in various functions (Security policy, IT operations, HIPAA compliance, etc.) and has worked with Federal healthcare systems and infrastructures since 2008. I have worked on IT and security architecture, facility workflow (to comply with HIPAA/PCI, etc.) FedRAMP, FISMA, and lots of other fun stuff. My twitter is full of sarcasm: ajohn76 My LinkedIn looks professional: www.linkedin.com/in/ajohn

Mark Kikta
(@B31tf4c3)

Mark Kikta is a Security Consultant with VioPoint which is located in Auburn Hills, Michigan. Mark supports a variety of operational security programs that includes vulnerability management security monitoring and incident response.

Rafal Los
(@Wh1t3Rabbit)

Rafal Los, Principal, Strategic Security Services with HP Enterprise Security Services applies over a decade of experience in various aspects of the security field to help clients meet complex security challenges. Focusing on strategic and tactical defensibility, Rafal assists clients with aligning security to the enterprise, developing operational efficiency, and measuring performance with effective KPIs. Rafal is a recognizer speaker, writer, blogger and contributor to open projects such as OWASP and the Cloud Security Alliance.

Kevin Riggs
(@ADubiousDude)

Kevin Riggs, Technical Architect Information Security Architecture Unum Group. Two decades in information technology covering ops, development and architecture. Experience from a two-man consulting business to a regulated 10,000+ employee enterprise.
http://blog.adubiousdude.com/

Matt Smith

Principal Security Analyst at Sword&Shield Enterprise Security.
Matt has been active in professional and technical security services for government and commercial clientele for more than 15 years. He is experienced in working all aspects of the system security life cycle from planning and design to implementation and testing.
At Sword & Shield, Matt performs network vulnerability assessments/ penetration testing utilizing a combination of commercial, open source, and custom software packages and assists in maintaining corporate knowledge on system vulnerabilities and penetration methods.
He is a graduate of Tennessee Technological University and holds the SANS GPEN, GCIH, GAWN, GWAPT and NSA IAM certifications."

ISSA
Information Systems Security Association
Middle Tennessee Chapter

The primary purpose of the Middle Tennessee ISSA Chapter is to promote the Information Security profession through education of its members and interaction with the community.

To promote the education of, and help expand the knowledge and skills of its members in the interrelated fields of information systems security, and information or data processing;
To encourage a free exchange of information security techniques, approaches, and problem solving by its members;
To provide adequate communication to keep members abreast of current events in information processing and security which can be beneficial to them and their employers;
To raise awareness of security issues and their resolutions in local businesses and the community.

WWW.ISSA-MEMPHIS

Jayson E. Street
(@jaysonstreet)

Jayson E. Street is an author of "Dissecting the hack: The F0rb1dd3n Network" from Syngress. Also creator of http://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. ;-)

Scott Thomas
(@secureholio)

Scott Thomas is a Information Security professional with over 14 years of experience in Information Technology. He is a Senior Security Consultant specializing in Vulnerability Management for VioPoint in Auburn Hills, Michigan and believes that you can learn something from every person you meet.

BSIDES NASHVILLE

Magenta Monkey Studio
MARYMCONLEY.COM

net Works
networks that work™

Net Works is a company that lives up to its name.

We build networks that work! We've developed a method (and reputation) for designing and installing computer networks that are successful. Our engineers and technicians are focused on delivering just what our name promises.

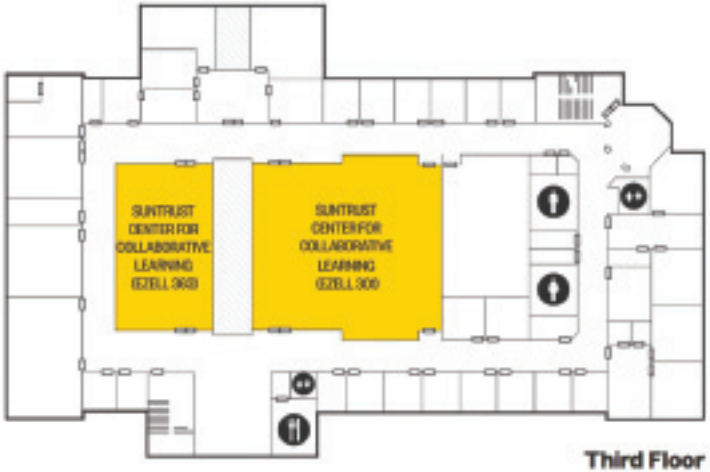
With fast, responsive IT solutions, our clients can focus on running their businesses with the assurance that their networks are reliable, secure and supported by an experienced technology partner.

Your IT solutions CAN be simple and cost effective. With Net Works, your company will save time and money with a more stable and usable computer network – done right the first time.

www.networksthatwork.net

Georgia Weidman
(@georgiaweidman)

Georgia Weidman is the Founder and CEO of Bulb Security, LLC, a security consulting and research firm. Georgia is a penetration tester, security researcher, and trainer. She has presented her work at top conferences around the world including the Black Hat Briefings, Shmoocon, Derbycon, and many others. Georgia has delivered highly technical security trainings to excellent reviews. Her work in mobile botnets and assessing the security posture of smartphones has been featured on news programs and in print. She was awarded a DARPA Cyber Fast Track grant to continue her work in mobile device security, culminating in the release of the Smartphone Pentest Framework (SPF) which allows pentesters to assess the security of mobile devices in an environment. Georgia holds an M.S. in computer science with emphases in secure software and information security as well as CISSP, CEH, OSCP, and NIST 4011 certifications.



First Floor

Registration .....Ezell Lobby
Information.....Center Hallway
Sponsors..... Room 107
Track 101..... Board Room
Track 418..... Room 136
Track 429..... Room 109

Third Floor

Opening Ceremony.....Ezell Room 301
Keynote.....Ezell Room 301
Lunch.....Ezell Room 301
Closeing Ceremony.....Ezell Room 301

TIME	ACTIVITY
08:00 - 09:00	Registration
09:00 - 09:15	Welcome to BSidesNashville
09:15 - 10:15	Name: Jack Daniel - Technical Product Manager at Tenable Network Security Talk: BSides, Harmonicas, and Communication Skills
10:15 - 10:30	Coffee Break

Time	INFOSEC 101 TRACK	INFOSEC 418 TRACK	INFOSEC 429 TRACK
10:30 - 11:30	Name: Eve Adams Talk: Attack Paths: Breaking Into Infosec From IT Or Other Totally Different Fields	Name: Russell Butturini Talk: Making Mongo Cry: Automated NoSQL exploitation with NoSQLMap	Name: Paul Coggin Talk: Bending and Twisting Networks
11:40 - 12:40	Name: Adam Len Compton Talk: Learn From Your Mistakes	Name: Matt Smith Talk: Buy Viagra!	Name: Mark Kikta Talk: Seeing Purple: Hybrid Security Teams for the Enterprise
13:00 - 14:00	**LUNCH**		
14:15 - 15:15	Name: Scott Thomas Talk: Beating the Infosec Learning Curve Without Burning Out	Name: Lucas Gates Talk: How do I hack thee? Let me count the ways	Name: Kevin Riggs Talk: Scaling Security in the Enterprise: Making People a Stronger Link
15:30 - 16:30	Name: TBD Talk: TBD	Name: Adam John Talk: Healthcare Security, which protocal?	Name: Georgia Weidman Talk: TBD
16:45 - 17:45	Name: Jayson E. Street Talk: Around the world in 80 Cons	Name: Salvador Grec Talk: Malware Analysis 101 - N00b to Ninja in 60 Minutes	Name: Rafal Los Talk: Succeeding with Enterprise Software Security Key Performance Indicators
18:00 - 18:30	**Closing Ceremonies**		
18:30 and Beyond	**After Party**		

Presentations

KEYNOTE SPEAKER:
BSides, Harmonicas, and Communication Skills
Jack Daniel (@jack_daniel):

Humans are storytellers, but we load up PowerPoint (and Keynote, etc.) with bullets and shoot to kill the imagination and interest of our audiences. In this conversation Jack will discuss how to use storytelling techniques to improve your communication and presentation skills; how to safely disarm your slide decks by removing bullets, and what to replace them with; when storytelling is appropriate- and when it isn't. Jack will share insights, tips, and tricks gained through years of study, personal experience (successes and failures), and practice. And, he will tell a story or two- just don't ask to sit on his lap while he tells them, that is just awkward.

Attack Paths: Breaking Into Infosec From IT Or Other Totally Different Fields
Eve Adams (@HackerHuntress):

So you think you want a career in information security, but you work in an IT function where you barely get to touch firewalls? Or you're a software developer who's interested in learning to write more secure code. Maybe you're not even in an IT function at all, but you'd like to learn about securing data in fields such as law enforcement, finance or health care. Where to begin? Seasoned infosec recruiter Eve Adams, Senior Talent Acquisition Expert at Halock Security Labs, gets these questions all the time - and she's helped people find the right "attack paths" to start careers in infosec, without much or any prior experience in the field. She'll walk you through techniques for self-study, networking, and identifying where exactly you want to go in the wide world of security, using entertaining and immediately actionable examples from the real world. There will be plenty to learn for security neophytes, as well as those already working in the field looking for insight on career development - and lots of time for lively, interactive Q&A!

Making Mongo Cry: Automated NoSQL exploitation with NoSQLMap
Russell Butturini (@tcstoolHax0r):

This presentation will discuss some of the inherent security flaws and weaknesses in NoSQL databases, with a particular interest and focus on MongoDB. The presentation will examine how NoSQL databases work, where configuration weaknesses exist "out of the box", and how web applications using NoSQL backends can be exploited.

NoSQLMap, a Python tool written for automatically stealing data from NoSQL databases and applications, will also be demoed.

Bending and Twisting Networks

Paul Coggin (@paulcoggin):

Learn about network attack vectors that an adversary can use to control, and influence network traffic flows and exfiltrate data by exploiting network devices and protocols in the LAN, WAN and Cloud. Defensive methods and techniques for monitoring and protecting against the outlined attack vectors will be discussed. This presentation explores advanced methods and techniques that penetration testers, network engineers and security auditors need to understand about network infrastructure and protocols.

- Strategies for attacking network infrastructure
- Undocumented method for tunneling IPv6
- Layer 3 LAN based MITM attack
- Methods for exfiltrating data from the core network infrastructure including MPLS core network infrastructure
- Router tricks that penetration testers need to know
- Often over looked network trust relationships, integration, dependencies and interdependencies
- Features hackers know about routers that need to be understood by auditors and network administrators.
- Switch security the Achilles heel of networks everywhere and what to do about it.
- Ensure that you know when someone is twisting and bending your network infrastructure to suit their purposes
- Advanced service provider technologies that be utilized by an attacker to enable data exfiltration and WAN based
- MITM attack vectors, manipulate and override routing paths

Learn From Your Mistakes

Adam Len Compton (@tatanus):

The presentation is a fun little talk about various mistakes that either I or colleagues of mine have experienced/made and how we learned from our mistakes to make us better security consultants. All names have been changes to protect the guilty. :) Hopefully this presentation helps people to realize that it is okay to make mistakes, as long as you learn from them and move on.

How do I hack thee? Let me count the ways

Lucas Gates (@lucasgates)

Most medium/large organizations spend a considerable amount of time and resources securing their organization. Are they getting the biggest bang for the dollar? Find out by hearing how we walked into a bank and got the manager's password and other fun stories!

Salvador Grec (@grecs): Malware Analysis 101 - N00b to Ninja in 60 Minutes

Knowing how to perform basic malware analysis can go a long way in helping infosec analysts do some basic triage to either crush the mundane or recognize when its time to pass the more serious samples on to the the big boys. This presentation covers several analysis environment options and the three quick steps that allows almost anyone with a general technical background to go from n00b to ninja (;)) in no time. Well … maybe not a "ninja" per se but the closing does address follow-on resources on the cheap for those wanting to dive deeper into the dark world of malware analysis.

Healthcare Security, which protocal?

Adam John (@ajohn76)

It is no secret that most healthcare systems are behind the curve both in technology, but also security in relation to the business world. One of the biggest issues is that there is no one option that is a panacea, and to add to the woes are three major types of healthcare organizations (payer, Federal/State, and provider). To add to the confusion are multiple sub-groups, executives that do not understand the needs, and a concept of protecting data is diametrically opposed to this world where sharing it has been a cornerstone for centuries. I plan to take a quick (101 level) dive to see the various issues with each of these 3 groups, and some simple foundational steps to start patching up the wounds. Maybe I'll pull in some audience participation with question/answer to set things up.

Seeing Purple: Hybrid Security Teams for the Enterprise

Mark Kikta (@B31tf4c3)

The militaries of the world conduct wargames in order to increase their readiness in the event of an actual incident. The job is to provide security for their respective nations. For those of us responsible for the security of organizations, why should our methods be any different? Protecting any sufficiently sized infrastructure is just like protecting a virtual country; there can be everything from minor skirmishes by untrained personnel (skiddies) to attacks by

SOPHOS

IT security products have become as complex as the networks they're trying to secure. At Sophos we know that the solution to complexity is not more complexity. We tackle security challenges with clarity and confidence, knowing that simple security is better security.

We began producing antivirus and encryption products nearly 30 years ago. Today our products help secure the networks used by 100 million people in 150 countries and 100,000 businesses, including Pixar, Under Armour, Northrop Grumman, Xerox, Ford, Avis, and Toshiba.

As IT networks grow in complexity, we're focused on keeping IT security simple and reliable. We know that a proper security strategy must include networks, servers and devices—all devices—managed easily through the cloud.

www.sophos.com

nation states (APTs) to attacks from within (insider threat). It is paramount that security teams plan, prepare, and execute mitigations for these events. By combining both red and blue team operations in your organization, you can develop comprehensive security exercises that will not only help you identify holes in your existing procedures, but also help you develop new ones all while keeping your team at the top of their game. This talk will explore blueprints for creating such a team, how to integrate it into your existing hierarchy, and how to make it fun!

Succeeding with Enterprise Software Security Key Performance Indicators

Rafal Los (@Wh1t3Rabbit):

Enterprise software security has been a hot topic for over a decade, yet enterprises of all sizes continue to fail at explaining measurable gains, but why? The answer lies in how and what is measured. Success begins with realistic, business-aligned KPIs which can be effectively measured to demonstrate improvement, or lack thereof. Come learn what, and how to effectively measure software security.

Scaling Security in the Enterprise: Making People a Stronger Link

Kevin Riggs (@ADubiousDude):

Employees' knowledge, understanding and application of security continues to be a significant challenge in a continuous maturity process of security and risk management. Increases in numbers of employees and complexity of business complicate security implementations.

We will discuss establishing a program to scale out security and risk management principles, frameworks and architecture to any size business to empower solution delivery that effectively applies security and risk management. Real world examples presented will

SystemFrontier

Noxigen LLC was founded in 2012 to build solutions that solve enterprise problems around systems management, compliance and access control. With a laser focus on making your company more efficient, you can expect great customer service and a product that continually improves to meet customer needs.

System Frontier is a Privilege Management solution which takes a different approach than most products from other vendors. It gives IT admins the ability to easily delegate granular rights to specific objects on a server using role based access control.

All rights are centrally managed and fully audited to make it much easier to see what was done on any given system and by who. Eliminate the paperwork. Eliminate admin rights.

Try System Frontier FREE for 30 days
noxigen.com/Software.aspx

include strategic targeting of partners and fostering a culture of change from C-level leadership throughout the organization. Time will be given to documenting and reporting business value.

Buy Viagra!

Matt Smith:

Are you part of the booming online pharmaceutical business or would like to be? This talk revolves around the interesting web command and control processes used by members of one or more pharma affiliate organizations, as uncovered by Sword&Shield on an actual intrusion case. And how your web sites could be compromised in this very same way and you don't even know it!

Around the world in 80 Cons

Jayson E. Street (@jaysonstreet)

This is a talk on perspectives. I step outside of mine to see hacking around the world though different views.
We will explore how companies who publish reports help skew the global perspective. We will look at how people from different parts of the world see hacking/ information security from their own perspective. We will hear a few tales of what I saw through my perspective of a stranger in a foreign land. We will then explore a small slice of history of a few hackers to gain a better perspective of where we have been, where we are now and where we are heading.
This talk was not only created to entertain and enlighten the conference attendees to take a step back and look at what they themselves are a part of. It was made for them to share with friends, family and coworkers. So people on the outside could get a better understanding of what a hacker truly is and why being one is such a great thing to be!

Beating the Infosec Learning Curve Without Burning Out

Scott Thomas (@secureholio)

So you have made the decision to get into Infosec and you're excited to begin your new adventure. Great! What area interests you the most? You know that "Information Security" has many jobs right? Maybe you started out with a IT background. Maybe you were an electrical engineer. Maybe you just decided "that hacker stuff" sounded

like fun. Whatever brought you here, you are going to have the same issues that affects many people starting a new career...where do I learn everything? Do you go the certification route and end up with alphabet soup on your resume or perhaps take the road of higher education and obtain a degree with a fancy name? Are either of them required or just a way to get your foot in the door?
This talk will be an intro to what the speaker (who still wants to learn more) did to get into the industry and a couple tips to avoid burnout with the plethora of jobs and learning paths out there. It will also identify how he was able to find the people that helped him along the way. This talk is mostly geared towards new people starting their career in Infosec.

TBD it's a Suprise.
Georgia Weidman
(@georgiaweidman):
Arn't you courious? You should go.

B-Sides Nash Training Review . Get in Early next year !

Yeasterday Georgia Weidman hosted a training session: **"Hands-on Penetration Testing with Metasploit"** during Bsides Nashville: This course will gave hands-on experience in many facets of penetration testing. It briefly touched on the basics of using Kali Linux as well as programming and scripting. We studied the Metasploit Framework before using it and supporting tools to simulate a penetration test against target virtual machines. Starting with information gathering, The class moved through the phases of penetration testing. The class will began with basic, easily exploitable vulnerabilities, but also covered the latest client side issues being exploited in the wild. This course heavily focused on post exploitation techniques such as privilege escalation, lateral movement, and pivoting. We will study advanced techniques such as bypassing anti-virus and IDS systems. The basics of developing exploits manually rather than using tools will be covered. We will turn our custom exploits into Metasploit modules. Finally, we will take a look at the rapidly developing field of mobile hacking.

The course finished with a live capture the flag environment where students were able to test what they have learned.

SPONSORS

Last but by no means least, we want to thank our sponsors, Kickstart Backers and individuals who purchased tickets as well as the volunteers and participants who helped put together this awesome security conference .We could not have run this event without you!

LBMC Security & Risk Services
PLATINUM SPONSOR

ISSA
GOLD SPONSOR

tenable network security
BRONZE SPONSOR

netWorks
SOPHOS
LUNCH SPONSORS

System Frontier
PARTY SPONSOR

PentesterAcademy
MEDIA PARTNER

Magenta Monkey Studio
GRAPHIC DESIGN

BSIDES NASHVILLE

B SIDES
NASHVILLE
© B-Sides Nashville 2014