
PROGRAM
2018
BSIDES
NASHVILLE
BsidesNash.org
@BsidesNash

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

BSides Nashville 2018

Welcome to BSides Nashville for 2018!

On behalf of the Organizing Committee, volunteers, speakers and sponsors we are pleased you are here. Here we are 5 years and now an OFFICIAL 501c3! Can you believe it? And we are busting at the seems and working on ways to have more people here next year. We are amazed and overwhelmed by your support. We would like to thank our sponsors. Without their generosity, this conference would not exist. Each of our sponsors bring resources and enthusiasm to this event. A special thank you goes out to Lipscomb's College of Computing and Technology for providing the perfect space and atmosphere, for a fifth year. We are all students of the security craft, and we welcome the new students and the more experienced to help us in our learning.

We have intentionally avoided tight schedules in the plan and we want all of you to relax, share, and connect. We believe that the real value of a BSides conference 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'll let y'all borrow one) and relax. Go check out the Phish Bowl. Minecraft is back as are some new fun things for kids of all ages. Brought to you by people of the community, we give them the space so check out their hard work. New this year there is also a resume and interview workshop, sign up for a slot to help or be helped. Please check the room for walk in times.
Once again we are excited to bring you great speakers from around the US and many from TN and nearby Kentucky. Please show your appreciation, as they are volunteers and came at their own expense to share their knowledge.

Come see, meet, talk… and leave inspired. Volunteer for next year! Bsides Nashville is a labor of love and many hands make for light work. All of the work leads up to a great con. If you would like to see Bsides Nash continue in all it's awesomeness and can spare an hour or 2 a week, we could use you in planning our 6th and Bsides Nashville, in its new location.

KEYNOTE SPEAKER: Ladi Adefala

Ladi Adefala is a passionate cyber security professional with a broad range of expertise that spans multiple security domains including cyber security strategy, solution architectures, security risk assessments, cyber threat intelligence and research and cyber security training. Adefala's background in information technology and security began with stints at Red Hat Consulting, AT&T and World Wide Technology Inc., and his credentials include an MBA from Washington University and multiple industry certifications. Mr. Adefala has served in a variety of strategic technical and leadership roles that span several disciplines including enterprise network, mobility and advanced cyber security solutions. As a FortiGuard Labs cyber security expert with Fortinet, Adefala engages in industry thought leadership and threat research initiatives. These include strategic, tactical and operational threat intelligence. He has been invited to share his research and cyber security thought leadership at several events including NASA, BSidesLV. Adefala's area of active research is deep learning neural networks. He also serves as Adjunct Faculty at Webster University's Masters of Science – Cyber Security Program, where he engages participating students in the domains of Critical Infrastructure Protection (CIP), network forensics, malware analysis and reverse engineering.

Barrett Adams

Barrett is also a penetration tester and security professional with experience performing a variety of red team assessments. His focus has been on assessing externally facing networks, where he has developed a number of useful automation scripts to search for, consolidate, and organize a company's internet presence. In addition, his portfolio includes a number of other attack tools such as an Outlook (OWA) address harvesting script and several spear phishing payloads designed to bypass email filtering and sandbox technologies.

Timothy De Block

Timothy De Block is a senior software security engineer for a Nashville based company. He has a blast in his day-to-day role building processes and improving the security mindset of those around him. He enjoys presenting, podcasting, and long evenings of Overwatch.

Russell Butturini

Russell Butturini has been in IT and information security for the last 15 years and currently is the senior security architect at a top 20 CPA firm. Every once in a while, he cobbles together some badly written but cool Python code that people seem to like and presents it at various conferences such as Defcon, Derbycon, and various BSides. His tool, NoSQLMap, has been starred 655 times on Github (which is 654 times too many), and was also published in "The Hacker Playbook 2".

Dustin Childs

Dustin C. Childs is a part of Trend Micro's Zero Day Initiative (ZDI) and handles communications for the group. In this role, Mr. Childs creates, implements, and oversees communications programs, both internal and external, that promote the work of ZDI and its researchers. This includes editing and writing security analysis and supporting collateral from researchers associated with ZDI. The ZDI team augments Trend Micro's security products with 0-day research through a network of over 3,000 independent researchers around the world. Mr. Childs is also responsible for providing insight into the threat landscape; competitive intelligence to the research team; and providing guidance on the social media roadmap. Part of his role also includes speaking publicly and promoting the research produced by the ZDI. He has presented at numerous conferences including BlueHat and THOTCON. Prior to Trend Micro, Mr. Childs worked in response communications as a part of the Microsoft Trustworthy Computing (TwC) group. He also worked as a security program manager in the Microsoft Security Response Center (MSRC) and is a veteran of the U.S. Air Force. With over 20 years in information security roles, Mr. Childs approaches issues with an understanding of the different real-world implications for various IT roles.

Patrick Coble

Patrick Coble is an independent EUC and Security Consultant working around Nashville, TN. Patrick has worked in IT for 20 years and as a consultant for over 10 years. He is a recognized expert in Virtualization, EUC solutions and Security. He has deployed hundreds of VDI deployments using both Citrix and VMware solutions all over the southeast. Patrick is working to expose and close the gaps in VDI solutions when it comes to security. He helps with Red and Blue teams to gain access and secure VDI deployments.

Adam Compton

Adam Compton has been a programmer, researcher, professional pentester, father, husband, and farmer. Adam has over 15 years of programming, network security, incident response, security assessment, and penetration testing experience. Throughout Adam's career, he has worked for both federal and international government agencies as well as within various aspects of the private sector.

Brian Contos

Brian Contos has over two decades of experience in the security industry. He is a seasoned executive, board advisor, security company entrepreneur and author. After getting his start in security with the Defense Information Systems Agency (DISA) and later Bell Labs, Brian began the process of building security startups and taking multiple companies through successful IPOs and acquisitions including: Riptech, ArcSight, Imperva, McAfee and Solera Networks. Brian has worked in over 50 countries across six continents. He is a strategic board advisor for multiple companies including Cylance and Appdome. He has authored several security books, his latest with the former Deputy Director of the NSA, spoken at leading security events globally and is a Distinguished Fellow with the Ponemon Institute. Brian frequently appears in the news and has been featured in CNBC, C-SPAN, Fox, NPR, Forbes, Wall Street Journal, The London Times and many others. He most recently appeared in a cyberwar documentary alongside General Michael Hayden (former Director NSA and CIA).


Don't be a fool!
Security Awareness
is no joke!
SAC
the security awareness
COMPANY
Call or email us today! +1.727.393.6600 (CST) | SACinfo@thesecurityawarenesscompany.com

Rodney Hampton

Rodney Hampton is an attorney and security consultant who has hacked out programs in Basic, Fortran, Pascal, VBA, PHP, Perl, Java, and -- most recently -- Python. Rodney got his first computer, a Commodore Vic-20, in 1982 and was a computer enthusiast long before I.T. became his career. He now has 18 years of professional experience working his way up and over from web development to infrastructure and finally to security. Before joining a consultancy, Rodney was the Security Manager for a Fortune 500 oil and gas company. Rodney's formal education includes an Associate of Science degree in Business, Magna Cum Laude, a BA in History from The Ohio State University, and a JD, Magna Cum Laude, from Western Michigan University. He was admitted to the bar in 2011. Rodney is a Certified Information Systems Security Professional and he holds several other vendor-specific certifications.

Cindy Jones

Cindy brings over 20 years of specialized IT and security experience to her role of Principal Security Consultant with Rapid7. Cindy maintains a CISSP and MCP certifications. She has worked in multiple arenas including Federal, education, technology and healthcare and has a background in development, maintenance and management of information security programs. In her current role, Cindy assists clients in determining the most effective means of improving upon their information security programs. Cindy studied Psychology while in her home town of Los Angeles, and is currently enrolled with Western Governors University, earning a BS degree in Information Technology - Security. Cindy is actively involved within the information security community and volunteers her time by leading the registration team for BSides Las Vegas, volunteers for DerbyCon, and DEF CON. Her favorite color is purple and she doesn't use that as a security question.

Erich Kron

Erich Kron, Security Awareness Advocate at KnowBe4, is a veteran information security professional with over 20 years' experience in the medical, aerospace manufacturing and defense fields. He is the former security manager for the 2nd Regional Cyber Center-Western Hemisphere and holds CISSP, CISSP-ISSAP, MCITP and ITIL v3 certifications, among others. Erich has worked with information security professionals around the world to provide the tools, training and educational opportunities to succeed in Information Security.

Bryce Kunz

Bryce @TweekFawkes) loves researching and red teaming bleeding edge IT services. Bryce is currently the Chief Hacker & President at Stage2Sec.com where he released various open source tools (e.g. soMeta, lolrusLove, yupPhrasing, etc…) and has contributed several modules to open source projects (e.g. empire). Previously, Bryce has supported the NSA (network exploitation & vulnerability research), Adobe (built red teaming program for cloud services), and DHS (incident response). Bryce holds numerous certifications (e.g. OSCP, CISSP, ...), and has spoken at various security conferences (i.e. BlackHat, DerbyCon, BSidesLV, etc...).

Leo Meyerovich

Leo Meyerovich co-founded Graphistry to supercharge visual investigations. Over the last 15 years at UC Berkeley and various R&D labs, his research spanned the first security policy change-impact analyzer (2005), functional reactive web framework (2005), parallel web browser (2009), reasoning about the social foundations of programming languages (2012), and leading to Graphistry, the first GPU visual analytics language (2013). These projects helped start popular web technologies at companies including Mozilla, Facebook, and Microsoft, were awarded SIGPLAN's best research of the year, and received 2 best paper awards.

Qualys®

Continuous Security

Doug Munro

Doug Munro has been embedded in Talent Acquisition for more than fifteen years, beginning in agency Recruiting before moving into corporate roles. His talent pool immersion has included Software Engineers, Database Developers and Administrators, Network Architects and Engineers, Executives, and Cybersecurity Specialists in multiple disciplines. His experience encompasses both private and public sector customers, both actively recruiting professionals to fill key roles and leading teams of recruiters to elevate firms' Talent Acquisition capabilities. Doug's public sector experience includes securing top security-cleared talent for mission-critical efforts across dozens of Department of Defense and Intelligence Community entities. His current focus is Cybersecurity, identifying talent for Coalfire, a leading Cybersecurity services firm, in the areas of Risk and Vulnerability Assessment, Cyber Risk Advisory, Penetration Testing, and Cyber Engineering. As a proponent of community-based recruiting, Doug has participated in numerous events, speaking and offering resume and career advice at events like RecruitDC, BSidesLasVegas, BSidesDC, and the ISC2 CyyberSecureGov event, among others.

Chris Myers

Chris is an experienced penetration tester with 5 years in the information security industry. He's led a diverse range of red team assessments, from internal networks, to spear-phishing exercises, to web and mobile applications. These assessments have given him exposure in a breadth of industries (pharma, finance, healthcare, technology, etc.) through which he's developed a unique perspective of the current information security landscape. His areas of interest include exploit development, offensive security training and education, and automation and tool development.

John O'Keefe-Odom

John O'Keefe-Odom is a Chattanooga area web programmer who works in a variety of server-side and client-side languages. He has combat experience with operating mobile, encrypted, wireless RATT (Radio Automatic Teletype) systems during Desert Storm. His contemporary career includes a project which involved the discovery, identification and removal of a remote access trojan on a UNIX production system which was being pawned for use as an illegal authentication theft and carding server. His recent projects include programming to support communications among databases, server-side programs, and PLCs.

Frank Rietta

Frank Rietta is a web application security consultant, software developer, author, and speaker. He is a computer scientist with a Masters in Information Security from the College of Computing at the Georgia Institute of Technology. A blue team fan, he is passionate about teaching on how to design custom web-based software to be secure. Additionally, he is a contributor to the security chapter of the 7th edition of the "Fundamentals of Database Systems" textbook published by Addison-Wesley.

Kathleen Smith

Kathleen Smith (moderator) in her capacity as CMO and Outreach Lead for CyberSecJobs.Com and ClearedJobs.Net has coached thousands of job seekers and employers on how to better connect and work together to achieve the mutual goal of employment. Kathleen presents at several security conferences each year on recruiting and job search. Some of the conferences she has presented at as a sole presenter or a moderator include BSidesLV, BSidesTampa, BSidesDE, FedCyber, Cyber912 and CyberSecureGov. Kathleen firmly believes that giving back is the best way to move forward and volunteers in many capacities; she is the Director, HireGround, BSidesLV's two day career track; Women in Cybersecurity, National Conference Planning Committee, Cy ber912 and Women in Cybersecurity Celebration Planning Committee. Finally, Kathleen is well respected within the recruiting community; is the co-founder and current President of recruitDC, the largest community of recruiters in the Washington DC area.

Nancy Snoke

Nancy Snoke currently works as a security consultant focusing on web and mobile applications. In the past she has been the senior software engineer responsible for web application security at PGAC, and a penetration tester for Cisco Systems. Nancy has previously spoken at Derbycon, NOLACON, Skydogcon and Bsides. She got her undergraduate degree in Computer Engineering at Tulane University, and her Masters in Computer Science at University of Illinois Urbana-Champaign.

Phoenix Snoke

Phoenix works as a private security consultant specializing in networks security and hardware. Phoenix has previously spoken at NOLACON, Skydogcon, and Bsides.

Michael St. Vincent

Michael St. Vincent is Chief Information Security Officer at The Cosmopolitan of Las Vegas, supporting the overall IT risk management program for the luxury casino and resort. St. Vincent joined The Cosmopolitan in May 2015, spearheading initiatives such as information security strategy and direction, implementation of security policies and The Cosmopolitan in May 2015, spearheading initiatives such as information security strategy and direction, implementation of security policies and standards and shaping the use of tools and processes, while ensuring

appropriate controls of technology. With more than two decades of experience as a leader within his field, he has developed, implemented, and led programs across Canada, Chile, Colombia, India, the United Kingdom, and the United States. St. Vincent holds an MBA, has been an active Certified Information Systems Security Professional (CISSP) since 1998 and maintains additional certifications such as CISA, CISM and CRISC. He has participated on the SANS GCIA Advisory Board, Microsoft's CSO Council, the FBI CISO Academy, and in local groups, providing support to encourage a stronger profession.

Judy Towers

CounterIntelligence Special Agent (6 yrs), Judy Towers provided weekly SAEDA briefings for new incoming unit soldiers and for yearly awareness training requirements. Judy received an Army award for the presentation's effectiveness in engaging the audience and enhancing self-awareness of the threat. After leaving the Army, Judy started a civilian career in information security as: domain admin for a global company, an IT manager implementing an incident response system, Fraud department investigating people stealing company services, and now a Cyber Threat Intelligence Analyst, augmented by a 2nd Master's Degree in Cybersecurity and Computer ForensicsChampaign.

Bruce Wilson

Bruce is an Enterprise Architect at Oak Ridge National Laboratory, where his roles include leading identity and credential management. By original training, he is a chemist and statistician, but wandered into doing high throughput research, and found himself drowning in data. He started writing tools to help manage and analyze his own data, then extending those tools for others, and then moving fully into enterprise IT (so that scientists can science).

Magen Wu

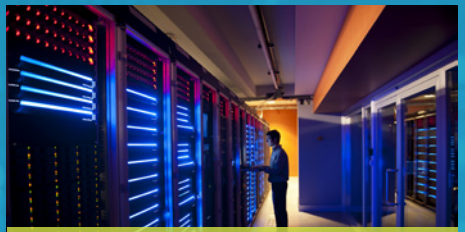
Magen Wu is a Security Consultant with Rapid7 with almost 10 years of experience in the technology industry. Wu is currently pursuing her master's in Organizational Psychology with the intent to apply its principles to security practices and training. She also currently co-organizes BSides Seattle and the mentor track at BSides Las Vegas.

ISSA
Information Systems Security Association

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 **one of the nation's top 35 information technology schools** on your team. Contact Brett Ramsey at **brett.ramsey@lipscomb.edu** for more information.

LIPSCOMB UNIVERSITY | COLLEGE OF COMPUTING & TECHNOLOGY

technology.lipscomb.edu

ENDGAME.

The Only Agent You'll Ever Need

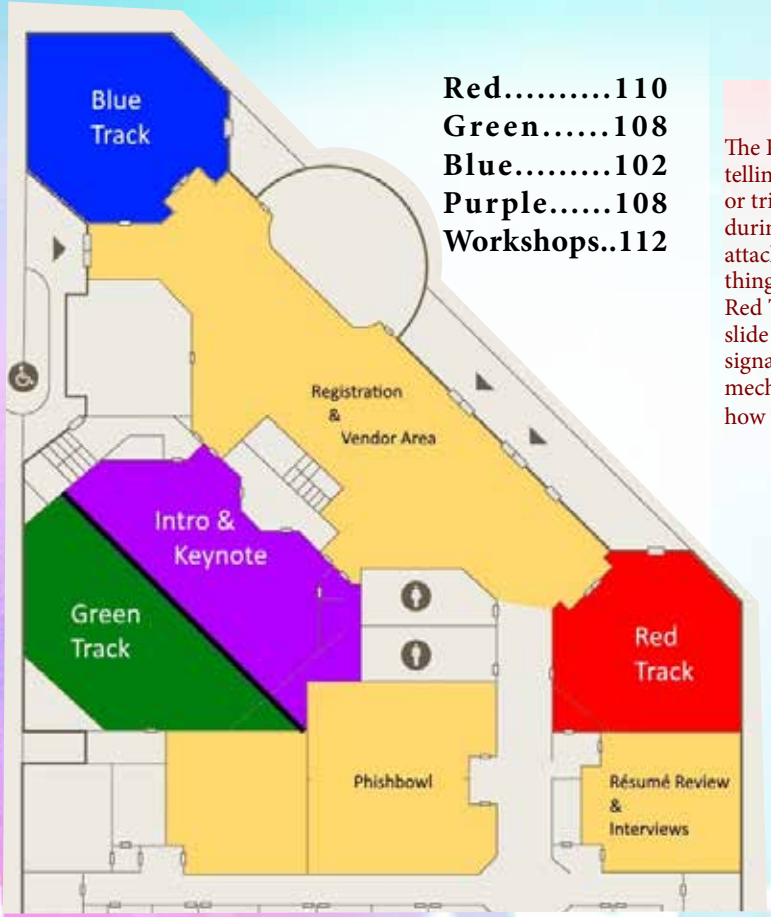
ENDGAME ARTEMIS

- Replace AV
- Stop ransomware, malware, phishing, and fileless attacks
- Automated threat hunting

Visit our table to learn more!

HIPAA COMPLIANCE · PCI DSS · amtso · AV comparatives

Schedule



Red.....110
Green.....108
Blue.....102
Purple.....108
Workshops..112

RED Track

The Red track is for technical talks telling us about new attack vectors or tricks learned while pentesting or during research. We all love a good attack talk and to hear about the latest things, but we have a challenge to all Red Team talks, include at least one slide telling the defense side about signatures for the attack, defense mechanisms to protect against it or how you could have been caught.

BLUE Track

The Blue track is for talks about defense. We all know attacks are sexy but many of us are on the defensive side. This track is to tell us about Defensive tactics, how a program was built with duct tape and bubble gum or other stories from the defensive trenches.

GREEN Track

The Green track is geared toward newcomers to the Infosec industry and professional growth.

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: Ladi Adefala
10:15 - 10:30	Coffee Break

Time	Green	Red	Blue
10:30 - 11:30	**ITwitterbots, Russian Influence Operations, and You** *Rodney Hampton*	**Blue Cloud of Death: Red Teaming** *Azure Bryce Kunz*	**Deploying Microsoft Advanced Threat Analytics in the Real World** *Russell Butturini*
11:40 - 12:40	**Learning to Hack the IOT with the Damn Vulnerable Habit Helper IOT Device** *Nancy & Phoenix Snoke*	**Security instrumentation: be the hero getting value from security** *Brian Contos*	**Changing Who Writes the Queries: High-Leverage IR with Visual Playbooks & Visual Graph Analysis** *Leo Meyerovich*
12:45 - 13:30	**LUNCH**		
13:30-14:00	**Closing Remarks, Prize Giveways and Other Awesome**		
14:00 - 15:00	**Community Based Career Activities or How Having Fun Can Help You with Your Career** *Kathleen Smith, Cindy Jones, Doug Munro Magen Wu*	**Hillbilly Storytime - Pentest Fails** *Adam Compton*	**Hacking the Users: Developing the Human Sensor and Firewall** *Erich Kron*
15:10 - 16:10	**See the ID Rules Before Us: FAL IAL AAL eh? Aaaagh!!! How, How, How, How?** *Bruce Wilson*	**SAEDY: Subversion and Espionage Directed Against You** *Judy Towers*	**What Happens in Vegas: Near Real-Time Vulnerability Visibility** *Michael St. Vincent*
15:45 - 16:10			**Growing Up to be a Infosec Policy Driven Organization** *Frank Rietta*
16:20 - 17:20	**Hacking VDI 101** *Patrick Coble*	**Adding Simulated Users to Your Pen-testing Lab with PowerShell** *Chris Myers, Barrett Adams*	**Evaluating Injection Attack Tools Through Quasi-Natural Experi-mentation** *John O'Keefe-Odom*
16:55 - 17:20	**Social Engineering for the Blue Team** *Tim De Block*		
18:30 - 21:00	**After Party at: Pour House Burgers, Bourbon and Brews**		

KEYNOTE :

Know Your Why

09:15 - 10:15

Oladipupo (Ladi) Adefala

The two most important days of your life are the day you were born and the day you find out why". This quote by Mark Twain reminds us of the importance of knowing our why. Sometimes our why can get fuzzy as we go through life. My story of knowing my why begins with a song and continues with a series of unexpected events. Join us for the BSides Nashville keynote for a time of music, some dancing and stories that speak to our hearts as well as our mind

Twitterbots, Russian Influence Operations, and You

10:30 - 11:30

Rodney Hampton

After the 2016 Presidential election, congressional investigation revealed something that has long been known in the intelligence community. Foreign powers, particularly Russia, have been using social media to conduct influence operations. TN_GOP was one of the twitter bots discovered to have been controlled by Russia. This talk will examine some of the investigative work done by NATO and the Atlantic Council's Digital Forensic Research Lab on these bots, show the author's own python code written to increase twitter following / social reach and how easily such code can be weaponized for far more sinister uses (OSINT/SIGINT, influence operations, and kinetic targeting). Finally, additional code will be shown that interacts with users on the Russian site VK (their equivalent of Facebook). Attendees will, hopefully, develop more heightened OPSEC practices and skepticism in their use of social media.

Green Track

Learning to Hack the IOT with the Damn Vulnerable Habit He lper IOT Device

11:40 - 12:40

Nancy Snoke, Phoenix Snoke

In this talk, husband and wife team Phoenix and Nancy Snoke introduce the Damn Vulnerable Habit Helper (DVHH) IOT device. DVHH contains a hardware device, mobile application, web application and associated api calls / network communication. DVHH was built to make getting started in IOT hacking more accessible to everyone. This talk will introduce the DVHH. We discuss why we created DVHH, how it is archtiected, and how to get started using it. As hardware hacking seems to be the sticking point for many on hacking IOT, this talk will include Phoenix talking a random audience member through a live hardware hacking demonstration on the DVHH device (chosen at random).

A parts lists and instructions / schematic will be given for the hardware inclined who wish to build their own device. All necessary parts can be bought for under 30 dollars. Several prebuilt hardware devices will be available for demo or purchase for those who do not want to build the device themselves.

Community Based Career Activities or How Having Fun Can Help You with Your Career

14:00 - 15:00

Kathleen Smith, Cindy Jones, Doug Munro, Stacey Banks

At 40, everyone is obligated to take that mid-life look at one's self and take an account of where they have been, where they wanted to go, the bitch that is reality, and where they will probably end up. After sailing my way through the the IT and infosec worlds from techie to interacting with C-levels, it's been an interesting ride with potholes and great opportunities. I'll opine about what I've found to really matter, what doesn't, and what you need to do but you don't want to. I don't have all of the answers, but I have a map that will help you get where you really should go.

See the ID Rules Before Us: FAL IAL AAL eh? Aaaagh!!! How, How, How, How?

15:10 - 16:10

Bruce Wilson

In July 2017, after many months of public comment and open discussion on github, the US National Institutes of Standards (NIST) released revision 3 of special publication 800-63: Digital Identity Guidelines. This was a huge revision that separated out what used to be a single level of assurance into three separate components: Identity Assurance Level, Authentication Assurance Level, and Federation Assurance Level. It gets rid of things many thought were counterproductive, like arbitrary password complexity requirements and time-based forced password changes. It notes that a one time password via SMS has some value, but is also weak (though they backed away from calling it "deprecated"). It also adds some very interesting concepts, like "additional authenticators" and "supervised remote enrollment".
For some, NIST 800-63 is something we have to follow. Others can look at it as guidance and a source of best practices. For all, it's a fairly long set of documents describing a complex subject (digital identity) that's at the absolute center of getting security right. So, let's spend some time working through NIST 800-63, look at these changes and new concepts, and see what separating identity from authentication from federation can mean for us.

Hacking VDI 101

16:20 - 16:50

Patrick Coble

Do you have a VDI deployment or a client that does? VDI Deployments are in over 90% of all the Fortune 1000 companies and are used in almost all industry verticals, but are they secure? The goal of most VDI deployments is to centrally deliver applications and/or desktops to users internally and externally, but in many cases their basic security recommendations haven't been fully configured. This talk will review the basic design of the top two solution providers, Citrix and VMware. We will go over these solutions strengths and weaknesses and learn how to quickly identify server roles and pivot. We will also examine some of the major attack points and their defensive counters.

Social Engineering for the Blue Team

16:55 - 17:20

Tim De Block

Social engineering is not just for red team. It's a powerful tool that the blue team can use to improve security within the organization. Have you ever struggled to get another department to take security seriously? Have you ever been frustrated that security takes a back seat to other priorities? Social engineering is the answer. We can be better at getting our goals and objectives accomplished by improving how we interact with others.

This talk will provide tools and techniques to build better

relationships. We'll talk about what we're doing right and what we're doing wrong. How to use social engineering to build rapport with your co-workers. We'll talk about verbal and electronic communication techniques, body language, going the extra mile, and appreciation. Learning the tools and techniques of social engineers will help you build better relationships and influence others into a better security mindset.

Red Track

Blue Cloud of Death: Red Teaming Azure
10:30 - 11:30
Bryce

On-demand IT services are being publicized as the "new normal", but often times these services are misunderstood and hence misconfigured by engineers which can frequently enable red teams to gain, expand, and persist access within Azure environments.
In this talk we will dive into how Azure services are commonly breached (e.g. discovering insecure blob storage), and then show how attackers are pivoting between the data & control planes (e.g. mounting hard disks, swapping keys, etc...) to expand access. Finally we will demonstrate some previously unknown techniques for persisting access within Azure environments for prolonged periods of time.

Security Instrumentation: Be The Hero Getting Value From Security
11:40 - 12:40
Brian Contos

You have many security products, probably too many. But you are still not secure because it's nearly impossible to know if your security products are actually doing what you want. Through live network and endpoint attack demonstrations, see how to use attack behaviors with Bartalex, Vawtrak, Mimikatz, PowerShell, Tunneling and others to validate your actual security products are working. See startling statistics, based on real-life case studies, that illustrate how ineffective many organizations, some with massive security budgets and teams, actually are because of a lack of validation. See how you can turn these attacks into an opportunity to instrument more effective security.

1.You will be able to identify your own assumption-based security risks.
2.You will be able to distinguish new ways of diagnosing security effectiveness across people, processes and technology.
3.You will see how security effectiveness can be measured, managed and improved.
4.You will learn how to communicate security effectiveness to business and technical leaders.
5.You will be able to reproduce practical mechanisms to effect positive security change within your own organization.

Hillbilly Storytime - Pentest Fails
14:00 - 15:00
Adam Compton

Hearing about awesome new discoveries and astounding exploits are always fun, but what of those times when things just go wrong? Stop by and listen as I share stories of times I, and others, have made both hilarious and educational mistakes. All stores and events are true (but the names may have been changed to prevent embarrassment). Whether or not you are just starting in InfoSec, it is always important to remember

that mistakes happen, even to the best and most seasoned of analysts. The key is to learn from your mistakes and keep going.

SAEDY: Subversion and Espionage Directed Against You

15:10 - 16:10

Judy Towers

"Frequently, people who go along a treasonous path do not know they are on a treasonous path until it is too late", as per testimony from former CIA Director John Brennan, May 2017. The definition of social engineering (SE) is: "any act that influences a person to take an action that may or may not be in their best interest". Using an old US Army acronym called SAEDA, Subversion and Espionage Directed Against the Army, I will discuss how today's use of SE is essentially trade craft of espionage, commonly known as spying.
"There is no patch for an untrained user or even an experienced security professional who forgets, in the heat of the moment, to follow what they have been taught." Espionage is the practice of secretly gathering information about a foreign government or a competing industry, with the objective of placing one's own government or corporation at a strategic or financial advantage. Presenting case examples of military and industrial espionage will illustrate how tricks of the spy trade are parleyed against ordinary individuals every day. The ultimate goal is for individuals to become self-aware as today's cyber threat landscape is essentially 'them against you'.

Adding Simulated Users to Your Pentesting Lab with PowerShell

16:20 - 17:20

Chris Myers, Barrett Adams

Pentesting labs tend to have isolated boxes representing specific vulnerabilities. This doesn't do a great job of mimicking real world networks which have active users and network activity. We created a tool set to introduce simulated users to a lab environment which enables us to accurately model real world corporate networks and allows for additional attack vectors to be explored in a safe setting. During this talk we'll go over the major functions of the tool and showcase its capabilities with a live demonstration.

Blue Track

Deploying Microsoft Advanced Threat Analytics in the Real World

10:30 - 11:30

Russell Butturini

Microsoft Advanced Threat Analytics is a great tool you probably already own whether you know it or not, but all the talks on it have been about setting it up in a lab environment... Until now! This talk will be a totally unbiased, non-vendor speak look into experiences successfully implementing ATA in a large production environment, including what ATA is and is not, architecture, installation, tuning, and how to avoid certain "gotchas" along the way.

Abstract:

Introductions/Why give a talk on ATA? -An overview of Advanced Threat Analytics (What it is, and what it is not) -ATA architecture -ATA Center overview, deployment guidelines, and security considerations -ATA Gateway architecture and deployment -Overview of ATA incidents, reports, rules, behavioral analytics, and tuning. -Advanced usage of the ATA database for threat hunting -Troubleshooting and getting help -ATA alternatives for non Microsoft shops -Time for questions/comments

Changing Who Writes the Queries: High-Leverage IR with Visual Playbooks & Visual Graph Analysis

11:40 - 12:40

Leo Meyerovich

Incident response investigations are not living in the magical future Hollywood promised. Instead, when an incident comes up, understanding it generally still means searching through logs and jumping through different tool UI panels. Most likely, with notepad open. This talk shares our experiences in increasing leverage in the active investigation process through visual playbook automation and visual graph analysis. We'll focuses on initial high-leverage application of these ideas within IR. Visual graph analysis simplifies answering questions around incident scope, progression, correlations, and outliers. Visual playbooks solve how to quickly and reliably gather data around an incident and present it in an interpretable and actionable manner. We'll show how to combine these ideas to improve handling of malware, phishing, audits, and other common IR investigation tasks. Throughout, we'll demonstrate how to achieve these results by connecting traditional Splunk/ELK/Hadoop/graph stacks to Graphistry for query generation and data visualization.

Hacking the Users: Developing the Human Sensor and Firewall

14:00 - 15:00

Erich Kron

CEO Fraud, W2 Fraud and ransomware all have one thing in common, they are commonly spread by phishing attacks. Phishing attacks have made Ransomware a $1billion industry in 2016 with CEO fraud and W2 fraud right there alongside it. As the bad guys get better, we must step up our game as well. Users are often overlooked as tools in your security program. This session will discuss how you can turn your users in to effective attack sensors and human firewalls to keep your organization safe from social engineering attacks such as phishing, smishing and vishing and hybrids.

This session will discuss:

- Current phishing trends and scams
- The real goal of security awareness training
- Dealing with the politics of phishing your users
- Making your security awareness training count
- Dealing with repeat offenders

What Happens in Vegas: Near Real-Time Vulnerability Visibility

15:10 - 15:35
Michael St. Vincent

Real-time visibility to vulnerabilities can be extremely challenging, especially when you have a large network of mixed systems. Without it, balancing remediation against non-stop gaming uptime is a difficult bet to place. The key to monitoring a continually changing set of hosts in the environment is having a strategy to complete deep scans within tight timelines. In this talk, a flexible and automated approach is presented from work in Las Vegas. A scanner scheduling method was developed to perform efficient vulnerability scans, detect new hosts, determine when to add more scanning nodes, and report change as it happens. Whether using a commercial or an open source platform, learn how one "revolving scan" strategy enables an immediate view.

Growing Up to be a Infosec Policy Driven Organization

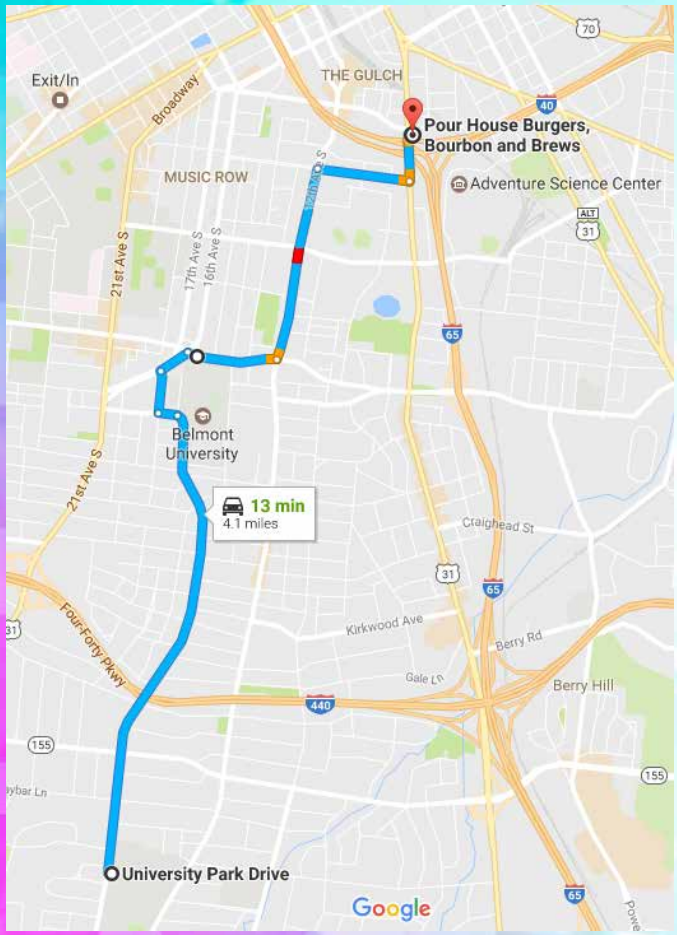
15:45 - 16:10
Frank Rietta

Internet software as a service (SaaS) companies with the need to protect private consumer information do not start out as a big organization with defined roles and separation of duties. They start out as a couple of founders, then a developer or two, and grow from there. Then as the team grows there may suddenly appear an external security requirement when a possible enterprise contract inquires about the status of the written information security policy or for other information about the organization's security governance. Now the core team that may still only be a few developers and a small business team need to define and adopt policies or forego the business. This talk is about that journey from being a small agile team to being one whose operations have documented security policy and procedures without needlessly overwhelming the business or operations.

Evaluating Injection Attack Tools Through Quasi-Natural Experimentation

16:20 - 17:20
John O'Keefe-Odom

Because breach is inevitable, the ability to investigate security compromises has never been more important. But, what makes someone good at finding and catching bad guys? Even most experts cannot fully articulate the tacit knowledge that makes them so good at what they do.
In this presentation, I will tackle that question by approaching information security from a cognitive psychology perspective to identify abstract tools that are commonly mastered by expert threat hunters. This will include discussions about framing the investigation process using the scientific method, curiosity as an x-factor contributing to success, the merits of thinking with a pivoting mindset, and more.
This talk should provide valuable insight to beginner and expert analysts alike. You should walk away with a more thorough understanding of how investigation expertise is a lot less about tangible software tools and much more about abstract tools inherent to the mind, and how to further your skills and career using that knowledge."



BSIDES NASHVILLE Party

Pour House Burgers, Bourbon and Brews
730 8th Ave S,
Nashville, TN 37203

Please Rideshare and/or use valet

Sponsored by:

Qualys.
Continuous Security

SPONSORS

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!

PLATINUM SPONSOR

PLATINUM SPONSOR

PLATINUM SPONSOR

PARTY SPONSOR

GOLD SPONSOR

SILVER SPONSOR

SILVER SPONSOR

SILVER SPONSOR

SILVER SPONSOR

SILVER SPONSOR

SILVER SPONSOR

FRIEND

FRIEND

no starch press

FRIEND

FRIEND

FRIEND

GRAPHIC DESIGN

ORGANIZERS AND STAFF

Lauren Rogers..... President
Geoff Collins .....Treasurer
Finn Breland ..... Secretary
Gabriel Bassett ..... Badge Wrangler and AV
Tommy Wolosin ..... Swagger Supplier
_NSAKey .....Phish the Hoopy Frood
RC -..... The Force
Jennifer Samardak .....Nerf Herder
Ryan Goltry .....Faithful Scout
Adrian Crenshaw .....Video Production

SPECIAL THANKS

Cameron Haan .....All the Things I'll Do Them
Brian Sommers .....Shirt Herder
Dakota Beverly ..... Techno Scion
Josh McVay .This space left intentionally blank
Tabitha Bassett ..... Asst Nerf Herder
Tim De Block .....Papparazo