PROGRAM
2019

BsidesNash.org
@BsidesNash

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

BSides Nashville 2019

Welcome to BSides Nashville for 2019!

On behalf of the Organizing Committee, volunteers, speakers and sponsors we are pleased you are here this fine spring morning. It has been 6 years and we are still going strong, better than ever, and with a new venue! It is also the 500th BSides event globally YIPPPEEE!!!!

Yes, you will need your walking shoes but we are hoping that more room will help us be less claustrophobic and besides, you need to get your steps in today anyway.

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 continuing to support us in using Lipscomb University as a venue.

We are all students of the security craft, we welcome the new students and the more experienced to help us in our learning. Just like years past, we have intentionally avoided tight schedules 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. We aren't in High School anymore. So, find your slow, southern drawl (we'll let y'all borrow one) and relax. Go check out the Phish Bowl, located in the Student Activity Center. We have lockpicking, the Mental Health Hackers helping us relax, various video games, and the resume review workshop. We bring this to you, for the community, by the community. Please check out their hard work.

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 7th BSides Nashville.

KEYNOTE SPEAKER:

Marcus J. Carey

Marcus J. Carey is the founder and CEO of Threatcare. He describes himself as a hacker who helps people not suck at cybersecurity. He started his technology voyage in U.S. Navy Cryptology and later went on to refine his knowledge while working at the National Security Agency (NSA).

John Askew

John Askew is a penetration tester, software engineer, and occasional public speaker. He is a founder and principal consultant of Graywolf, and has worked full-time in offensive security for over a decade. Outside of work, he prefers hobbies that don't involve a computer screen, such as outdoor running and playing music.

Karlo Arozqueta

(Director of Sales Engineering at Verodin) Karlo Arozqueta has not known life without a keyboard since 1985 when he got his first computer, a Commodore 64. Since that time he's watched the age of computers, networking, the Internet and Computer Security turn from hobbies to careers. He's run his own computer consulting company, a hard drive data recovery company, spent 7 years running the Incident Response team for a major US Federal Agency, and is currently the Director of Engineering covering the US Federal market for Verodin. In addition to volunteering as staff at several conferences (ShmooCon, DerbyCon, SkyDogCon), he has spoken at conferences both large and small (GFIRST, ISACA, IR 2017, BSides Springfield, and Outerz0ne to name a few) and is a dynamic and entertaining speaker, due in no small part to also being an amateur standup-comedian. He often combines comedy and his technical expertise into what he has dubbed "Edutainement" and has always managed to keep his audience engaged.

Casey Bohn

Casey Bohn is currently a High-Tech Crime Specialist with the National White Collar Crime Center where he is the course lead for the Dark Web/OSINT course, and has assisted with the development of multiple courses including: Dark Currency, understanding Digital Footprints, and Digital Evidence Basics for Judges and Prosecutors. Mr. Bohn previously served as both a public and private sector digital forensic examiner. A veteran law enforcement officer with experience in patrol, SWAT, and investigations; Mr. Bohn has primarily investigated technology involved crimes, many of which were conducted in an undercover capacity and served on multiple task-forces aimed at electronic crimes. During his career, Mr. Bohn has earned multiple certifications related to digital forensics and remains active in the community through various organizations.

David Branscome

David works with Microsoft Partners, helping them deploy the latest Microsoft technologies, including security controls in Office 365, Windows 10 and Azure. He's worked at Microsoft for 10 years in a variety of roles, including 6 years in the Microsoft Consulting Services and Premier organizations, supporting customers in the Commercial, Federal, State and Local Government, and Higher Education customers as they deploy and manage on-premises, online and hybrid Microsoft technologies. David holds numerous certifications, including CISSP, GCWN, CCSP, CySA+, PenTest+, CEH, Security+ and several dozen Microsoft certifications. David has been married for 27 years, has 4 children (3 boys and a little girl) and lives outside Raleigh, NC. For a vacation, David loves nothing better than to rent a house on the Outer Banks with an ocean view, a week of sunshine and no WiFi anywhere!

Rockie Brockway

Rockie has been in infosec over 25 years. His spiffy business bio is on his LinkedIn page (much spiff! very wow!). He is the Practice Lead for the Office of the CSO in TrustedSec's Advisory group, is the President of the non-profit organization Secure Cleveland, which produces BSidesCleveland, and enjoys making things out of wood.

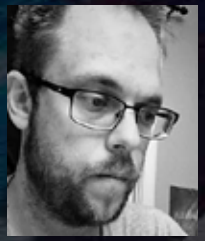
netWorks
networks that work™

ENDGAME.
MILITARY-GRADE ENDPOINT PROTECTION
THAT'S AS SIMPLE AS AV
EASY | ZERO TRAINING ENDPOINT PROTECTION PLATFORM
EFFECTIVE | STOP TARGETED ATTACKS ACROSS THE MITRE ATT&CK MATRIX
EVERYWHERE | FULL-FORCE, AUTONOMOUS PROTECTION
Visit our table to learn more!
MITRE
Gartner
virustotal
amtso
SE Labs
AV
ENDGAME.COM

Adam Compton

Adam Compton has been a programmer, researcher, professional pentester, father, husband, and farmer. Adam has around 2 decades 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.

David Cybuck

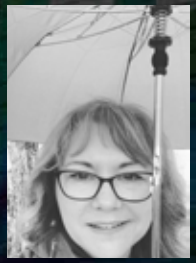


By day David brings application security into CI/CD (DevSecOps) or gets busy securing containers. He most enjoys supporting fellow professionals with coaching and positivity. And for the last 6 years he has been committed to applying a background in development, risk assessment, pentesting, auditing, monitoring, and a little DFIR to improving all software. He is a major believer in the OWASP SAMM, ASVS; using them at work. He is a minor contributor to the OWASP Proactive Controls 3.0. For fun he helps people breaking into InfoSec with MIRR workshops, and reads InfoSec books while moderating an online Infosec book club.

Mark Geeslin

Mark Geeslin is currently senior principal security engineer and director of application & product security at Asurion. Mark has been working in the software development and security industries for over 25 years in diverse environments ranging from high-tech security start-ups to Fortune 100 companies. In recent years he has directed AppSec programs for various leading technology firms in Silicon Valley. Besides his extensive experience as an engineer, Mark's expertise includes large-scale security assessments, penetration testing, threat modeling, static & dynamic software security analysis, and application security research. Mark has degrees in computer science and theology, and holds numerous security industry certifications.

Gigi Gridley



Gigi Gridley is a Threat Analyst based out of Huntsville, AL, with over 20 years of IT experience. Gigi's resume is full of words like firewall, sys admin, vulnerability analyst, and project lead. Her fried chicken is legendary. She has irritated plenty of users and managers, and would like you all to learn from her mistakes.

Keheira Henderson

I'm Keheira from Tennessee and the creator of Backpack Media, LLC. I'm a mobile applications developer that graduated from North Carolina A&T State University in Computer Engineering. When not coding a new app, I'm an avid reader, backpack collector, and gamer (I stream under the name mochila_ninja). I got into technology to work with robotics, but somewhere in college I fell in love with security and connected devices. In the future I aim to be a CTO and medical device security expert.

Rene Kolga

Rene Kolga, CISSP, has over 10 years of cybersecurity experience in the areas of endpoint protection, insider threat, encryption and vulnerability management. Rene run Product teams at multiple Silicon Valley startups as well as Fortune 500 companies, including Symantec, Citrix, Altiris, ThinAir and Nyotron. Rene earned his Computer Science degree from Tallinn University of Technology. He frequently speaks on security topics at industry conferences like BlackHat, InfoSec and (ISC)2.

Erich Kron

Erich Kron 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 US Army's 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.

Recorded Future

ANOMALI®

ANOMALI THREAT PLATFORM

ThreatStream®
Threat Intelligence Platform

Anomali Enterprise™
Threat Detection Engine

Bryce Kunz

Bryce Kunz (@TweekFawkes) loves researching and red teaming bleeding edge IT services. Bryce is currently the Chief Hacker & President at Stage 2 Security 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...).

Tony Lambert

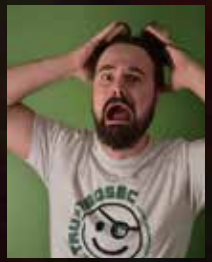
Tony is a recovering systems administrator that traded in chasing uptime for chasing adversaries. He is a geek that loves to discover how malicious tools work and learn about adversary techniques. Tony has completed a Masters of Digital Forensic Science from Champlain College and puts his skills to use hunting for malicious activity with Red Canary.

Isaiah Sarju

Isaiah Sarju is a red teamer. He has contributed to the Microsoft Security Intelligence Report, conducted numerous penetration/red team engagements, and taught students how to become top tier defenders. He plays tabletop games, swims, and trains Brazilian Jiu-Jitsu.

Ken Westin

Ken Westin is currently Senior Security Specialist at Splunk, helping organizations aggregate, analyze and operationalize disparate security data sources to identify and mitigate threats in various forms. In his past he has helped solve crimes with data, tracking stolen devices, breaking up organized crime groups, recovered stolen vehicles, even solved a violent carjacking, leading to the prosecution of dozens of criminals. He has presented at DEF CON, Black Hat, RSA, multiple BSides and security conferences around the world.



Rick Yocum

Rick has a 14 year history of both GRC consulting for a big-4 accounting firm, as well as managing and directing GRC practices for several large organizations in multiple different verticals. He is a Senior Security Consultant at TrustedSec.

CYBERSECURITY CAN BE BEAUTIFUL.

At Trend Micro, we've made cybersecurity an art form, orchestrating our proven foresight, XGen™ security strategy, and passionate people to secure your connected world.

Because when you can prepare for, withstand, and rapidly recover from threats, you're free to go further and do more.

That's The Art of Cybersecurity.

TheArtofCyberSecurity.com

TREND MICRO™

Phishing and business email compromise attack protection by Trend Micro, above and beyond native **Microsoft Office® 365® security**. Created with real data by artist **Matt DesLauriers**.

LIPSCOMB
UNIVERSITY

Leonovus

Schedule

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 - 10:15	Keynote at Student Activity Center
10:15 - 10:30	Coffee Break

Time	GREEN TRACK Ezell 301 - Third Floor	RED TRACK Ezell 241 - Second Floor	BLUE TRACK Ezell 147 - First Floor
10:30 - 11:30	Don't Be THAT Geek – How to communicate with users and management *Gigi Gridley*	Why your red team shouldn't be snowflakes *Isaiah Sarju*	Tell me to push my appsec left one more time: OWASP Proactive Controls *David Cybuck*
11:40 - 12:40	I Sold Out, You Should Too! Why I left Ops for Sales Engineering and Never Looked Back! *Karlo Arozqueta*	You Did What In My Bucket? Red Teaming GCP (Google Cloud Platform) *Bryce Kunz*	DevOps Application SecurityTeams for the Rest of Us *Mark Geeslin*
12:45 - 13:30	LUNCH		
13:30-14:00	Prizes		
14:00 - 15:00	Extracting the Attacker: Getting the Bad Guys Off Your SaaS *David Branscome*	A Methodology for Testing Tokens *John Askew*	What you know, what you have and what you are: MFA in the modern age *Erich Kron*
15:10-15:35	Bare-Knuckle Doxxing *Casey Bohn*	How Can I Become a Pentester *Adam Compton*	Att&ck Path Effectiveness *Rockie Brockway Rick Yocum*
15:40-16:10		Anatomy of a Nation-State Attack *Rene Kolga*	
16:20 - 16:50	Getting Started with Android Malware Analysis *Keheira Henderson*	White Collars & Black Hats: Bitcoin, Dark Nets and Insider Trading *Ken Westin*	Intelligence-Driven Testing with Atomic Red Team *Tony Lambert*
16:50 - 17:20			
18:30 - 21:00	After Party at: BLVD		

KEYNOTE :

Marcus J. Carey

In this talk, Marcus will talk about the past, current, and future state of hacking. Marcus will explore what we know about money, humans, and technology and what that means for our future. Marcus will discuss what we can do today to affect our future.

Green Track

Don't Be THAT Geek – How to communicate with users and management
Gigi Gridley

Users don't want to talk to "the IT department" unless they absolutely have to, because they've all had at least one experience of being talked down to.

But here's the thing - the IT department exists to help business users get their jobs done, and the IT department can't get money for upgrades and improvements without convincing management that it's good for the enterprise.

Those of us in technical roles don't usually get much training in soft skills like interdepartmental communication. Knowing how to talk to users is crucial to getting your own work done, so let's talk about how to make that happen.

I Sold Out, You Should Too! Why I left Ops for Sales Engineering and Never Looked Back!
Karlo Arozqueta

You started in entry level positions, paid your dues, maybe you worked in a 24/7 Operations center on the Blue team side or worked your way into an elite Red team. either way, congrats! You are now a skilled IT Security Veteran! Folks come to you to solve the problems no one else knows how to solve, and you are finally going to be rewarded for all you hard work by being promoted to.... MANAGEMENT! WOO!! Let's face it, most of us didn't spend our whole lives behind a keyboard, watching progress bars move to 99% and then sit there for an hour until it hit 100% to give it all up in exchange for managing people's vacation and thinking about their feelings. But there IS another way. You could choose to give up all that and move into a brave new world, one where the cake IS NOT a lie! You could sell your soul and go work in Sales as a Sales Engineer. Interested? Then this talk is for you! Come hear how the presenter took a leap of faith after SEVEN years in a 24/7 SOC as an Incident Responder and made the move to being a Sales Engineer. Now 4 years into it and it still has been the best frickin' job EVER! You'll hear why he did it, what questions to ask during the interview, what some of the jargon means, how to spot a good role from a bad one and why it could be the job that saves your life, marriage, and friendships (but I don't want to oversell it).

Extracting the Attacker: Getting the Bad Guys Off Your SaaS
David Branscome

The Microsoft Office 365 suite contains many applications that can help organizations do some amazing things. But every once in a while, a user in your organization will click on a link in an email, open a file or visit a malicious website, and their account will get compromised by an attacker. You can (and should) reset the user password, but is that enough? As you've probably guessed, if that was all you needed to do, this would be a VERY short session. The truth is, regaining control of a user account takes a little more effort to ensure the attacker isn't just temporarily inconvenienced. What are the steps you need to take to extract the attackers and get them off your SaaS? That's what I'll show you in this session, complete with demos. I'll also walk you through some sneaky areas where an attacker could potentially retain access, and show you how to shut it down. Finally, I'll show you some proactive steps you can take to keep these events to an absolute minimum. I can almost guarantee I'll show you some attack methods you haven't thought of before!

Bare-Knuckle Doxxing
Casey Bohn

An adversarial approach to risk identification and mitigation of an organizations most valuable assets; people. Specifically people and their open source digital foot print (MITRE ATT&CK 1266, 1275). Organizations participate in penetration testing and risk assessments, often times with a large chasm between the typical software/hardware solutions, and the ever present human element. With the proliferation of doxxing in the mainstream media, organizations and individuals need to be more aware of the adversary mind set and methodology, as well as the steps to simulate these attacks. Going beyond the attack simulation, organizations desperately need the ability to define and properly classify the associated risks, and identify steps to contain and remediate those risks.

This talk aims to give listeners an eye opening view into adversary simulation activities as it pertains to digital foot prints, but also will provide a crash course into the how and why of not only simulating the attack, but also highlighting methods to prevent and remediate our most important assets being compromised.

Getting Started with Android Malware Analysis
Keheira Henderson

Do you have a VDI The Android operating system has been around since 2008 and has also been open source from the beginning. Leaving things open source allows for a lot of apps to slide thru the cracks when it comes to security. At one point a flashlight app made the news for stealing user information when all it was suppose to do is turn on the camera light. This small incident has sparked tools that allow one to get into android malware analysis.

To my knowledge there is not a set tool that developers can use to make sure that their application can't be exploited. I spent years studying and building malware and now would like to help others to get into the malware analysis side in hopes that a general tool can be made for check applications before being published for consumer use. I'll take you thru setting up your environment and analyzing a controlled application apk. At the end of the talk you should leave excited to look more into Android malware analysis and the Android system as a whole.

Red Track

Why your red team shouldn't be snowflakes

Isaiah Sarju

Red teaming require the use of specialized tools. However, this should not exclude operators from using the same technology, adhering to the same procedures, and following the same policies as their colleagues throughout the organization. Some argue that this will prevent operators from executing on their duties. The contrary is true. With a few exceptions in place and thoughtful architecture considerations, treating red teamers as regular employees will improve their testing and reduce the risk that red teamers bring to organizations.

You Did What In My Bucket? Red Teaming GCP (Google Cloud Platform)

Bryce Kunz

Cloud services are frequently misconfigured due to their rapid adoption and engineers not fully understanding the security ramifications of different configurations, which can frequently enable red teams to gain, expand, and persist access within Google Cloud Platform (GCP) environments.

In this talk we will dive into how GCP services are commonly breached (e.g. discovering insecure cloud storage, SSRF vulnerabilities), and then show how attackers are expanding access within Docker & Kubernetes (K8s) environments (e.g. CVEs, insecure daemons). Finally we will demonstrate some unique techniques for persisting access within GCP environments for prolonged periods of time!

A Methodology for Testing Tokens

John Askew

Authentication and authorization are a key element of securing modern web/mobile applications, and most applications use a session token or some other type of token-based credential for such assertions. As a penetration tester, it can sometimes be very obvious when this process is broken, just by looking at the token value. But what if the token appears to be long enough, looks "random", and generally passes the smell test? Should we move on to other low-hanging fruit, or are there ways that we can dig deeper and still find vulnerabilities if we know the correct magic incantations?

In this session, we will present a methodology for analyzing token-based authentication systems from a (mostly) black-box perspective. We will cover how to break down token values and categorize them, how to identify potential vulnerabilities for further testing, and when to execute practical attacks against obfuscated, pseudorandom, or cryptographic token values. We will also release some proof-of-concept tools for performing analysis, and reference prior talks/tools that cover some specific attacks. Hopefully, you will leave this session with some new techniques for your application testing process. If you're tired of using burp sequencer and wondering if you're wasting your time, this session might be of interest to you.

How Can I Become a Pentester

Adam Compton

Stop by and take a seat while I discuss a couple different paths to a potential career in infosec. Does not matter if you are a student, an IT professional, or even someone interested in a career change; there is something here for everyone. I will be presenting my experience in understanding what current employers are looking for in new hires. Topics will include identifying most common roles for entry-level employees, recommendations on

education and training, and general advice on how to move your career ahead.

Anatomy of a Nation-State Attack

Rene Kolga

Among key advancements, this new OilRig attack campaign introduced a variety of new command and control (C&C) and data exfiltration capabilities using Google Drive, SmartFile, a file sharing and transfer solution, and an ISAPI filter to extend the functionality of Microsoft Internet Information Services (IIS) servers. In total, the attackers used about 20 different tools – some were off-the-shelf, dual-purpose utilities, while others were previously unseen malware. Leave this presentation armed with technical details of how sophisticated attackers operate along with knowledge that can help security professionals deal with this threat actor in the future.

White Collars & Black Hats: Bitcoin, Dark Nets and Insider Trading

Ken Westin

We know criminal hacking is big business, over the past decade, we have seen criminal syndicates get creative with ways of generating revenue, through markets selling stolen credit cards, selling of tools and services and more recently ransomware. With the rise of popularity in Bitcoin, there has been an increasing interest from those in the financial sector in the pseudo-anonymous currency as well as underground markets and sites sharing information via hidden services in the Tor network and other platforms. Financially savvy white collar criminals now have increased access to criminal hackers who can target, steal and share nonpublic data about companies, this paired with the anonymous nature of hidden services and Bitcoin reduces the risk of getting caught, but with large financial gains. In this talk we will review several cases where criminals have gained millions of dollars through compromising PR and legal firms and steps these organizations can take to protect this data.

TrustedSec
INFORMATION SECURITY + ADVISORY SERVICES CONSULTING
1.877.550.4728 | Info@TrustedSec.com

Blue Track

Tell me to push my appsec left one more time: OWASP Proactive Controls
David Cybuck

It may be true that pushing security left can stop us from developing breakable applications. And it matters how, and what, you push to developers. Even linters or other IDE tools are still not made for developers. Static code analysis output still needs to be translated into use cases or stories. It is meaningless when a tool reports SQL injection vulnerability. "The code meets the specification and design, those stories were closed 3 sprints ago, and QA and regression still pass; there is no bug in any of my use cases," said any developer. OWASP Proactive Controls are what we want to push left. They are a set of actionable security controls, going beyond developer training or static code scanning, that speak to developers. For the talk "our developers" write the OWASP Juice Shop. We will use examples and practice walking them through the OWASP proactive controls.

DevOps Application Security Teams for the Rest of Us
Mark Geeslin

Is it possible to do AppSec really well in a distributed DevOps environment at scale? Without hesitation, many in the security industry would answer with an emphatic "No!" Picture an organization with hundreds of projects in simultaneous flight, deploying continuously at any given time. Perhaps this is your organization? How can security be meaningfully injected into such apparent chaos?

Well, actually, it can be done. There are solutions that work and work well. In fact, you might even find that application security can be more robust than when you thought you had a handle on it – you know, back in the "good" ol' days of waterfall. One of the keys to making this work is a highly skilled, embedded AppSec team. Building and maintaining such a team, however, may appear prohibitively expensive and unmanageable. It need not be so.

This presentation will show you how to implement an AppSec program and develop an AppSec team that will fit well and function effectively within a large-scale distributed DevOps shop – without draining your budget! We will take you through our own journey of discovering what actually works (and what most certainly does not) within these challenging development environments, while providing specific details on the following: selling the program to upper management, building support throughout the organization, recruiting the AppSec team, training the AppSec team, interacting with the CISO's organization, impacting the product development culture and gaining influence, maintaining momentum, closing the gaps.

Doing AppSec properly in a distributed DevOps world won't be easy – nothing in life that's worthwhile ever is – but it is realistically achievable. If you are struggling with AppSec, this talk will give you hope for the future and a realistic plan for embedding security into your products more successfully than ever before.

What you know, what you have and what you are: MFA in the modern age
Erich Kron

A simple username and password are not enough to protect accounts and vital assets anymore. Time and time again, we see various types of accounts being compromised due to password reuse, phishing, smishing and vishing scams and overall poor password hygiene.

Throwing money at this problem doesn't make it go away.

Social engineering methods and the 'evil genius" cyber criminals behind the attacks are furiously innovating, keeping IT off-guard.

In this session we will discuss different types of multi-factor authentication (MFA) such as hardware keys, smart cards, SMS and application-based factors. The session will explain the differences between hardware-based One Time Passwords (HOTP), Time-based One Time Passwords (TOTP) and Personal Identity Verification (PIV) credentials. We will talk about the pros and cons of each, the vulnerabilities and the various ways that they can be leveraged to help protect accounts.

The session is designed for people interested in expanding their knowledge of multi-factor authentication and will cover:

- The damage being done through credential theft
- Hardware and software tokens
- PIV certificates and Smart Card login options
- Password vaults and MFA protections
- Protecting social media accounts

Att&ck Path Effectiveness

Rockie Brockway & Rick Yocum

Mitre's ATT&CK framework has many valuable features and characteristics, including the documentation of known threat actor groups and their associated attack techniques, as well as the breakdown of known attack techniques by tactic. One feature that is especially valuable is the cataloging of data sources that could be used to detect each individual attack technique. Roberto Rodriguez initially made the data sources to tools connection in his Threat Hunting blog posts "How Hot is your Hunt Team?" and "Ready to Hunt? First, Show me your Data!". By cataloging all of the data sources your current tools are able to look at (and potentially send to a centralized aggregator for ingestion), you can create a heat map of the known techniques, and how strong or weak your controls are per attack technique. This is effectively "Coverage", e.g. "I have these tools that should detect these techniques". But data sources and tools only represent one side of an effective Blue team, and does not take into consideration variables such as team talent per tool and talent constraints.

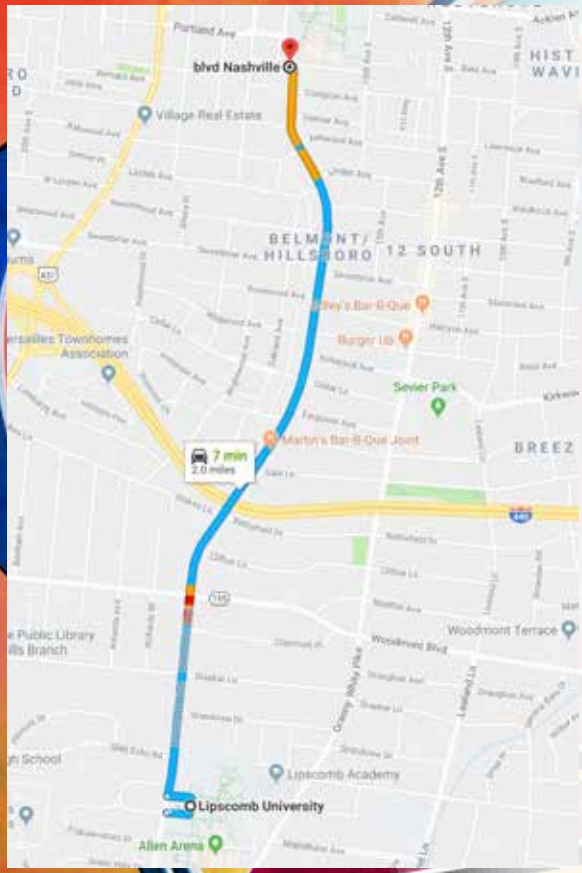
This talk represents the past year's worth of work developing an attack-path effectiveness tool using the Mitre ATT&CK framework, and will walk through the logic and process it took to go from Attack-Path "Coverage" to Attack-Path "Effectiveness".

Intelligence-Driven Testing with Atomic Red Team

16:00 -16:30

Tony Lambert

Time is short, resources are spread thin, and you have the responsibility to ensure your security investments deliver on their promises. Intelligence-driven testing shows how you can prove your controls work against real-world adversary techniques by consuming information and about adversaries and adapting tests for use from the freely-available Atomic Red Team project.



Party

BLVD Nashville

2013 Belmont Blvd
Nashville, TN 37212

Please Rideshare

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!

LIPSCOMB — PLATINUM SPONSOR

ENDGAME. — PLATINUM SPONSOR

Recorded Future — GOLD SPONSOR

ANOMALI — SILVER SPONSOR

TREND MICRO — SILVER SPONSOR

TrustedSec — SILVER SPONSOR

netWorks — SILVER SPONSOR

Leonovus — SILVER SPONSOR

ISSA — BRONZE SPONSOR

NYOTRON — BRONZE SPONSOR

no starch press — FRIEND

MENTAL HEALTH HACKERS — FRIEND

FOX PICK — FRIEND

Magpie Monkey Studio — GRAPHIC DESIGN

ORGANIZERS AND STAFF

Lauren Rogers..... President
Geoff Collins .....Treasurer and Vogon poet
Finn Breland ..... Secretary
Tommy Wolosin ..... Swagger Supplier
_NSAKEY.....Phish the Hoopy Frood
RC ..... The Force
Jennifer Samardak .....Nerf Herder
Ryan Goltry .....Prodigal Caffeinator
Cameron Haan .....CFP all the things
Josh McVay ..... CFP even more things
Brian Sommers .....Shirt Herder and left hand
Dan Quillen ..... Social media
Susan Richards..... Asst Nerf Herder
Tim De Block .....Papparazo
Gabriel Bassett ..... Head of Blockchains
Dakota Beverly ..... Website

© Bsides Nashville 2019