BSidesDFW 2018

Speaker Bios

In order of Presentation and Track

BSidesDFW 2018

Track 1 - 09:30
"The Mitre ATT&CK Framework is for all of us, and it is time to pay attention to it"
-- Michael Gough

Mitre has created the “Adversarial Tactics, Techniques & Common Knowledge” (ATT&CK) base to help security practitioners understand the actual techniques and tactics that adversaries use against us. The advantage of the ATT&CK base is it allows us to build a framework to understand how we might detect, respond, and prevent many of the tactics. The ATT&CK framework provides for a way for us to map what technologies and procedures we have, and then map any gaps that we have that then can be addressed.

@HackerHurricane | MalwareArchaeology.com

Track 2 - 09:30
"The Pentester Blueprint: A Guide to Becoming a Pentester"
-- Phillip Wylie

Pentesting or ethical hacking as it is more commonly known has become a much sought-after job by people in IT, InfoSec, or those just trying to get into the industry. In this presentation Phillip Wylie shares the blueprint for becoming a pentester. The presentation combines Phillip’s experience as a pentester and ethical hacking instructor to give attendees a guide to how to pursue a career as a pentester. Phillip shares what has worked for his students and people that he has mentored over his years as a pentester. This presentation covers the knowledge and skills needed to become a pentester as well as the steps to achieve them.

@phillipwylie | thehackermaker.com

Phillip Wylie is a Principal InfoSec Engineer on the Assessment Services Penetration Testing Team at U.S. Bank. Phillip is an Adjunct Instructor at Richland College teaching Ethical Hacking and System Defense. Phillip is a Bugcrowd Ambassador and the founder of The Pwn School Project. Phillip has 21 years of experience in InfoSec and IT and has performed pentests on networks, wireless networks, applications including thick client, web application and mobile. Phillip has a passion for sharing, mentoring and educating. This passion was his motivation to start teaching and founding The Pwn School Project, a free monthly educational meetup with a focus on hacking. Phillip holds the following certifications; CISSP, NSA-IAM, OSCP, GWAPT.

Track 3 - 09:30
"Cybersecurity Compliance and Legal Implications for 2019"
-- Jason Edwards & Griffin Weaver

Presenting legal and compliance topics relevant for today's cybersecurity professionals. This presentation will include discussions of current laws including NYDFS 500, NAIC Model Laws, GLBA and various topics from the FFIEC among others. Additional topics will include meeting regulatory requirements for risk assessments and a presentation of the various cybersecurity testing models for financial institutions such as the FFIEC CAT. Recent successful cyber-attacks have led the various federal and state legislative bodies to start increasing their regulation over the cybersecurity industry by including new requirements in new laws and regulations that cyber professionals should be aware of. The presenters will also discuss the best use of cyber security legal compliance in raising cyber awareness of executives who may not normally face heightened cyber compliance requirements. Finally, the presentation will be followed by a Q&A Session with the speakers who are experienced in regulatory cyber law and compliance.

@trackpads | www.jason-edwards.me

Jason Edwards has over 20 years of IT/Cybersecurity experience in various sectors such as military/government, insurance, security, banking, and energy. Jason currently works for USAA as the Compliance Director/Lead for Cybersecurity. Jason has earned the CISSP and both a B.S. and M.S. in Information Technology/Security. He serves as the principle compliance advisor for the USAA CISO and Information Security staff on regulatory cybersecurity compliance matters.

Griffin Weaver

Griffin is an experienced cybersecurity attorney and currently works for USAA in the Chief Legal Office as the principle advisor to the CISO. A preeminent lawyer and dynamic problem solver, Griffin assists USAA in identifying, evaluating and managing risks associated with technology and cybersecurity. He advises on federal and state cybersecurity laws, regulations and supervisory guidance. He provides extensive advice on cybersecurity risks, incidents and policy issues, including proactive cybersecurity readiness.

Track 1 - 10:30
"Windows Internals and Threat Hunting with Volatility"
-- Deepak Mahbubani

Introduction to Windows internals and memory analysis with Volatility memory forensics framework.

@datagoon

Track 2 - 10:30
"Developer Attack Surface"
-- Mark Morgan

This is not about XSS or SQL injection. This is about processes that surround development. As a former developer, I will be sharing areas of insecurity from a developer perspective that other might not be aware of from different backgrounds.

@_markmo_ | medium.com/@markmotig

Former developer of 18 years and currently a security engineer.

Track 3 - 10:30
"Rapid Fire Live Demos!"
-- Andy Thompson

Everyone knows you tempt the Gods when you attempt a live demonstration. With that said, this talk is series of rapid fire LIVE demonstrations of real-world attacks that organizations see on a daily basis. The goal is to present as many possible live demos of exploits and attacks as possible in the time allotted, one after another.

Attacks will include stealing hashes off the wire with Responder & Inveigh. Credential harvesting with LaZagne, Keystroke injection with Barcowned, Poison Tap, Bash Bunny, BadUSB, MouseJack and more!

Come for the hacks. Stay for the FAIL!

@R41nM4kr | www.MeteorMusic.com

With over 22 years in the industry, Andy, aka Rainmaker, Thompson is a information security consultant and National Manager of Customer Success at CyberArk Software, He specializes in Privileged Access Security and strategic guidance in risk mitigation with Fortune 100 enterprises. In his free time, he enjoys traveling the world with his family, and crashing his drone into random objects.

Track 1 - 11:30
"Ur Shellz Belong to AWS: Pentesting challenges against serverless environments"
-- Mark Clayton

Finding a remote code execution vulnerability to get shell on a S3 bucket? How about persistence on a Lambda or Google Cloud function? The game is different now and penetration testers should take heed.

Web architecture has moved from on-prem to DevOps CI/CD infrastructure deployment in the cloud and has now moved serverless...what the $&%# is serverless? Serverless is the application model that is changing the attack surface that is traditionally known by web application penetration testers, and allows developers to no longer focus on infrastructure provisioning, patch management, scaling, and much more. The burden of infrastructure is being offloaded to cloud providers, along with its associated security risks.

If your next pentest was a serverless application, how much of your existing attack methodology would still apply? Here we examine this application model and discuss exactly how the game has changed.

@bullz3ye | markclayton.github.io

Mark Clayton (Bullz3ye) is both an application security consultant and application developer, and can't seem to choose between the two. Professionally he is a security consultant for a very large corporation, and most likely developing React or Vue applications at night. Lately his primary focus is DevSecOps, where he blend the two. Before his current position, Bullzye served as a Security Consultant/Penetration tester for Occamsec. Prior to that he was in college.

Track 2 - 11:30
"Gray(log) is the New Black"
-- Megan Roddie

Graylog is a open-source log aggregation platform that is quickly gaining traction among the security community. This talk aims to show that by creatively utilizing some of the built-in capabilities, Graylog can transform from a log management platform into a SIEM, becoming a SecOps team's most powerful tool. The talk will start by defining the concepts of a log management tool vs a SIEM so, throughout the talk, a distinguished outline of how these customizations can be leveraged to make that transition. The different Graylog capabilities that will be leveraged to achieve SIEM status will be covered with a variety of examples of how they can be leveraged. Lastly, the shortcomings of the platform as a SIEM that users should be aware of from drinking from the Graylog kool-aid will be revealed.

@megan_roddie | blog.reconinfosec.com

Megan Roddie is a security analyst with Recon InfoSec. With previous experience in the public sector and a current position in the private sector, she has a variety of experience in different types of environments. With a love for public speaking, she has spoken at DEFCON, BSides Dallas, SOURCEConf, and various other conferences.

Track 3 - 11:30
"The Secret Weapon to Fight InfoSec FUD"
-- Olivia Stella

FUD (Fear, Uncertainty & Doubt) runs rampant in information security on a daily basis. Sensationalized claims leveraging stolen data or a simple misconfiguration are manipulated to make a headline. The science becomes so obscure that the true findings falls through the cracks. How do we get out of this vicious cycle? The secret weapon to fight FUD is provided from two points of view: the researcher and their target. As a researcher, how can you ensure your findings are taken seriously and not tagged as FUD? As a company or area under the eye of the research community, what can you do to not make the situation worse and become better respected.

@OliviaCurls

Olivia Stella is a senior security analyst for a US airline. In her current role, she focuses on aviation security and vulnerability management including pen testing and bug bounty. She has over ten years of experience in software development and information security. Previously, she worked at an in-flight entertainment company in product security supporting incident response, risk & compliance, and as the bug bounty lead. She holds a bachelor's degree in computer science, masters in software engineering, CISSP & CISM. When she's not wearing her security hat, she loves to curl and is an avid toastmaster. (That's right, ice curling.)

Track 1 - 13:30
"Singing the Blues: When Blue Team Kicks the Red Team's Arse"
-- Tinker

We often hear of the exploits of malicious actors and red team penetration testers. We constantly hear "There's always a way in! Everything can be hacked! You're fighting a losing battle! We're so 1337!". But what about those stories of when Blue Team stops an attacker cold? When Blue Team wins?

This is their story, Blue Team's story, as told by an attacker who went up against the best and was beaten.

Hear the Red Team "Singing the Blues" as they go through stories where the Blue Team detected, responded, contained, and caught the Red Team. We'll go through specifics on the Blue Team actions and provide key technical, procedural, and methodological take-aways on what actually works to stop the attackers.

@tinkersec | www.tinker.sh

Tinker is a penetration tester who conducts full scope red team ops, targeted penetration tests, & purple team co-ops. Tinker has built pentesting practices from the ground up, managed red teams, and is currently the Red Team Technical Lead for a Global Fortune Corp. Prior to this, Tinker served in the SOC trenches. Prior to that, Tinker served in the USMC.

Track 2 - 13:30
"Radio hacking 101: a case study in how to DoS the global APRS network"
-- Michael West

Many radio protocols have very little security, as they were designed when equipment to transmit was expensive and difficult to obtain. With the advent of SDRs, cheap radios, and of course the internet, these protocols are wide open to attack. In this talk, we'll discuss the fundamentals of radio hacking and apply these to the Amateur Packet Radio Service. We'll discuss possible attack avenues and ways to disrupt the entire global network. Conditions permitting, we'll also demonstrate a live, localized attack on the Dallas APRS repeaters. We'll tie this in to an overall discussion of how to get started hacking your favorite RF protocols.

@t3hub3rk1tten | mwe.st

Michael West, aka T3h Ub3r K1tten, is a National Technical Advisor at CyberArk who enjoys combining his software dev background with infosec to build tools for others. Michael presented "barcOwned" at DEF CON 26, has spoken at many BSides events around the country, and talks regularly at Dallas Hackers Association. His interests include OSINT, amateur radio, and scanning long barcodes on the beach.

Track 3 - 13:30
"Pseudorandom Meta Threat Intelligence. TL;DR - Lessons Learned from the Verizon Data Breach Investigation Report"
-- Walter Abeson

You've heard about it, you've seen it cited, you may have even printed it, but have you actually read the Verizon Data Breach Investigation Report (VDBIR) in its entirety? If not, no worries! While the experience of curling up with a nice libation and the scintillating 70 pages of the VDBIR is quite enticing, come hear a distilled version. Learn about the latest attack vectors, who the current cast of malicious actors are, and discover how to bolster your security posture against today's threat landscape. From human to technical exploits, internal to external agents, acquire the knowledge that's necessary to defend yourself against the threats that matter most.

@thesaltr

Walter Abeson is currently a Systems Engineer with RSA NetWitness, focusing on digital forensics, incident response, and threat hunting. Walter thrives at detecting anomalous behavior in both endpoint and network environments. Prior to joining RSA, Walter was the Technology Manager for Black Hat, responsible for the NOC and overall security posture. Walter continues to serve as staff for the Black Hat NOC and is also a goon at DEF CON. When not behind a computer, Walter enjoys photography, reading, and spending time outdoors.

Track 1 - 14:30
"Vigilante Forensics"
-- Litmoose

Armed with the knowledge of law enforcement requirements, this talk will enable cybersecurity practitioners to provide assistance to stalking and harassment victims.

So often, victims feel unsure of how to file a police report, the information needed to do so, and how to mitigate the ongoing negative situation as it exists.

Real stories, digital forensic practices for multiple devices, police process and a bit of opsec – this presentation will detail how to pivot in a unique active attacker situation and make your community a safer place.

@Litmoose

Litmoose is a Senior Digital Forensics and Incident Response Analyst for Fortune [REDACTED] Company in the DFW area. She has a master’s degree in Digital Forensics, did hard time in a SOC, and has a background in Medical Forensic Investigation (read: autopsies and bone identification). Favorite past time is stopping bad people from doing bad things.

Track 2 - 14:30
"Herding Happy Sheep - Securing an Open Environment"
-- Chris Mercer

It has been proven time and again that humans can't be trusted. So, we lock them down by removing permissions. Not only does this tend to upset users, but it inevitably creates more work for admins, such as having to intervene to install applications or making exceptions to policy for legacy applications. But what happens when the user finds a loophole? What happens when the admin is the bad guy? Or when someone disables that one little control, just for testing(tm), but forgets to turn it back on?

This talk will provide a high level, theoretical overview (backed up by some real world examples) of methods organizations can use to take a different approach to securing sensitive data. Using guide rails and automation, it will explore methods of giving freedom back to users and developers while your admins work on more important things. Your CISO will finally be able to get a good night's sleep knowing that his data is as safe as it could be, even if a compromise occurs.

@zaimorkai

Chris has been in the IT and infosec fields since the early 2000s. He is a US Army combat veteran with multiple overseas tours. He has served in system admin, security analyst, and penetration testing roles. He holds current OSCP and CISSP certifications, among others. Chris currently works in Dallas as a security architect, and also teaches cyber security courses at Richland College.

Track 3 - 14:30
"Dora Explores the Fascinating World of Spreadsheets!"
-- DoraTexplorer

People love spreadsheets. Macros and formulas are an easy way for non-coders to construct simple programs with a visual mini-database. Because of the widespread, everyday use of spreadsheets, people tend to trust them. Many applications also offer interaction via spreadsheets/CSV files (e.g. upload multiple lines, download as a spreadsheet, etc.). The popularity, implicit trust, integration into web applications, and extensive functionality combine to make a powerful vector of attack for red teams. This talk focuses on web app/spreadsheet interactions and how malicious actors could take advantage of client- and server-side coding issues to perform attacks ranging from XSS to RCE using spreadsheets.

@doratexplorer17

Dora's been exploring applications and systems in an official capacity for around 5 years. She's worked with institutions ranging from large investment banks to small libraries to identify and remediate flaws and provide training to developers. GWAPT certified. Actually 12 lizards stuffed into a human suit.

Track 1 - 15:30
"Dockerized Tooling for IH/IR"
-- Chris Rooney

This will cover what Docker is, what containers are, and why they are extremely useful in supporting incident handling and incident response activities. A base laptop with no installed security tools will be used for malware analysis. This will show the benefits of using containerized versions of security tools to support incident response and incident handling. Incident Response tools are usually built, deployed and maintained before there is an incident. A considerable amount of effort can be spent in maintaining dozens of laptops with all the tools a team may need in DFIR/IH. Too often it is discovered during an event that tools have stopped working. Kernel and Library updates can cause tools to fail when needed most. Systems updates, and inconsistent package updates can cause a team to have several different versions of the same tool running. Dockerized applications can be spun up extremely quickly. There is no lengthy install or configuration effort needed, meaning equipment can be swapped on the fly. When updated security tools come out, all analyst get access to the tools at the same time. This ease and quickness allows great flexibility in minimizing failures due to system updates, equipment failures, and even analyst skill gaps.

@Renegade0x6

Manager of security engineering, reformed manager of security operations, reformed chief of cyber network defense, and causer of general mayhem.

Track 2 - 15:30
"Staying Offensive: The Changing Landscape of Offense"
-- Tim Medin

Defense is changing and offense has to adapt accordingly. In this talk Tim will discuss the changes in the landscape he’s seen in his decade of experience in offense and what you can do to be more offensive. The goal of offense is to emulate real world attackers so the defenders can test the technology and better respond to attacks. Help the blue team by being more offensive.

@TimMedin | redsiege.com/blog

Tim Medin is the founder and Principal Consultant at Red Siege, a company focused to adversary emulation and penetration testing. Tim is also the SANS MSISE Program Director and a course author. He is the creator of the Kerberoasting, a technique to extract kerberos tickets in order to offline attack the password of enterprise service accounts.

Track 3 - 15:30
"Community Panel"
-- Q/A Panel

Meet leadership members of the DFW Infosec Community. Discover the diversity of organizations available to you all year round for growth and networking. It takes a village to rear a security professional and DFW has that in spades.

@DFW_InfoSec | @utdcsg | @Dallas_Hackers | @ISSAFortWorth | @DC214DFW | @OWASPDallas | @Hack_FtW | @SchoolPwn | @ntxissa | @isc2DFW | @ntxcsg | @0Dayallday

@CryptoPartyDFW | DFW DFIR Lunch Meetup | Dallas Cloud Security Meetup | @NorthTexasCSA | Infragard North Texas | @gdiDFW | @TheLab_ms | @dallasmakers

Track 1 - 16:30
"Reverse Engineering Ransomware - A Guided Tour"
-- Wesley McGrew

This presentation ditches PowerPoint for a slide-less walk through the internals of malicious software. Using the GandCrab ransomware as an illustrative example, Dr. McGrew will demonstrate for attendees the approach, techniques, and thought processes that are involved in extracting the capabilities and design of malicious software in the absence of source code. Those who are getting started in reverse engineering are often frustrated by overwhelming complexity and a lack of direction/defined-processes. In this demonstration, Dr. McGrew will demonstrate techniques for planning "what to do first/next" and making progress in a large or complex binary. The purpose of the demonstration is to give attendees with no RE experience an exposure to the interesting puzzle-solving aspects of reverse engineering.

@McGrewSecurity | hornecyber.com

Dr. McGrew serves as Director of Cyber Operations for HORNE Cyber. Wesley specializes in penetration testing, vulnerability analysis, reverse engineering of malware, and network traffic analysis. He is a frequent presenter at DEF CON and Black Hat USA. He teaches a self-designed reverse engineering course at Mississippi State University, using real-world, high-profile malware samples.

Track 2 - 16:30
"Building an Empire With (Iron)Python"
-- Jim Shaver

This talk discusses porting Python payloads to Windows using a little known, former Microsoft project. It explores offensive uses of .Net and Python on Windows and how to reduce attack surface on .Net payloads.

@elitest | jimshaver.net

Jim Shaver is a penetration tester and security researcher.

Track 3 - 16:30
"Community Panel (cont.)"
--
