BSides Atlanta 2010 PROGRAM

Start	Track 1 – In the Trenches	Track 2 – In the Watchtower	Track 3 – In the Mix	Bonus Exclusives: Panels & Training
9:30	Keynote - Jack Daniel			
10:00	Rob Ragan - Lord of the Bing: Taking Back Search Engine Hacking	Gary Palgon - A New Approach to Enterprise Data Security: Tokenization	Logan Kleier - SANS Top 20 Critical Controls Implementation	False Starts: How to Improve the Atlanta Security Community's Start:Exit Ratio - Interactive panel
10:30				
11:00	Dave Shackleford / Rick Hayes- Testing Exfiltration: Recreating Outbound Evil	Martin Fisher - Why We Suck at Incident Response	Nick Owen - Securing Remote Access with 2 Factor and Open Source	Information Security and the Modern College Campus - Interactive panel
11:30				
12:00	Lunch			
1:00	Aldrich de Mata / Christopher Elisan- Malware Packing and More	Thomas Cross - Unauthorized Internet Wiretapping: Exploiting Lawful Intercept	Todd Merrill - Protecting PHI with Encryption for HIPAA compliance	Training Seminar: Wireless Penetration Testing - Hosted by Errata Security
1:30			Taylor Banks - Letting go of Control: A 12-Step Program for Embracing the Cloud	
2:00	Dave Kennedy / Eric Smith - Strategic Penetration Testing	Tony UV - Applying Application Threat Modeling Beyond the Conceptual Hype	Brian Wilson - Intro to DOCSIS and Cable Modem Operations	
2:30			Michael Woolfe - How to Get Someone Else to do Your Job	
3:00	Chris Nickerson - Top 5 Ways to Steal a Company	Erik Peterson - The Long Con of Automated Dynamic Web Application Security Testing	Daniel Frye - Basics of Securing PeopleSoft Architectures	FALE: Locksport Group Training & Demonstration
3:30				
4:00	Mike Doyle - Pivoting Arbitrary Tools with Socket Proxy	Peter Hesse - Security Policies: The Next Generation	Karthik Rangarajan - Browser Add-Ons That Steal	
4:30	Gal Shpantzer - Security Domination via Hard Drive Isolation	Mike Rothman - Information Security 2011: Gaze into the Crystal Ball	Daniel Peck/Nidhi Shah - Demystifying Web Malware	
5:00				
5:45	Closing Reception			
7:30				

BSides Atlanta 2010 PROGRAM

EXCLUSIVE BONUS: PANELS

False Starts: How to Improve the Atlanta Security Community's Start:Exit Ratio
ISS is the poster child for security startups. Started by a teenager, grew to hundreds of millions in revenue, went public, then acquired. Since then, dozens of security companies have been started in Atlanta but few have reached a successful outcome. Part of the success of Silicon Valley is the ability to create two types of companies: 1) billion dollar independent 'pillar' companies and 2) high growth companies that can quickly prove out their value in terms of technology, revenue and customers and then become attractive M&A targets for larger technology companies. Out of dozens of security companies started in Atlanta over the last decade, we've only created one 'pillar' and a handful of 'exits' with many others still working to determine their growth path or some to even stay afloat. Dozens of other companies had good ideas and good people but did not reach the finish line. In this interactive panel, we explore what entrepreneurs and the Atlanta community need to do to increase the 'start-to-exit' ratio. This session will be led by:

- Dr. Paul Judge, CRO & VP, Barracuda Networks (@pauljudge)
- Nick Owen, CEO, WiKID Systems (@wikidsystems)
- Chris Rouland, Endgame Systems

Information Security and the Modern College Campus
This is an un-moderated interactive panel about the issues related to securing assets and setting policies for modern college campuses. This discussion will explore what it is like to operate a network in such an environment, war stories, new challenges and where it is going over the next 1-3 years. This session will be led by:

- Brad Judy - Information Security/Office of Information Technology - Emory University and Healthcare
- James Blanton - SSCP, Technical Services Manager ASaP - Kennesaw State University
- Michael Carroll - Systems Support Professional V - Kennesaw State University
- Stephen Gay - ITS Associate Director - Information Security Office – Kennesaw State University Information Security Officer

TRACK 1: IN THE TRENCHES

Name: Rob Ragan @sweepthatleg
Title: Lord of the Bing: Taking Back Search Engine Hacking from Google and Bing
Abstract: During World War II, the CIA created a special information intelligence unit to exploit information gathered from openly available sources. One classic example of the team's resourcefulness was the ability to determine whether Allied forces had successfully bombed bridges leading into Paris based on increasing orange prices. Since then OSINT sources have surged in number and diversity, but none can compare to the wealth of information provided by the Internet. Attackers have been clever enough in the past to take advantage of search engines to filter this information to identify vulnerabilities. However, current search hacking techniques have been stymied by search provider efforts to curb this type of behavior. Not anymore - this demonstration-heavy presentation picks up the subtle art of search engine hacking at the current state and discusses why these techniques fail. Several new search engine hacking techniques will be demonstrated that have resulted in remarkable breakthroughs against both Google and Bing. New tools will be demonstrated, along with the first ever "live vulnerability feed", which will quickly become the new standard on how to detect and protect yourself against these types of attacks.

Name: Dave Shackleford @daveshackleford & Rick Hayes @ISDPodcast
Title: Testing Exfiltration: Recreating Outbound Evil
Abstract: For years, security professionals have worried about protecting the perimeter, as well as systems and applications, from external threats. Insider threats have become much more prevalent now, as have stealthy sophisticated attacks and malware. Much to-do has been made of solutions like DLP and IPS, but are they really able to defend you from sensitive data and attacker communications *leaving* your network? In this presentation, we'll walk through a methodology you can put to use for simulating outbound data leakage and attacker communications scenarios. Traffic generation tools, obfuscation and tunneling techniques, and simulated bot and stealth malware comm channels will be covered. Fun for the whole family, guaranteed.

Name: Christopher Elisan @tophs and Aldrich de Mata
Title: Detecting Packed Malware: Looking at Packer Identifiers and Malware Packers
Abstract: Problems arise for the malware researcher when malware uses packers to compress and pack a binary file. Packed binaries evade detection of antivirus vendors and make the analysis of malware difficult for the researcher. This issue can be solved by first identifying which packer was used by the malware to pack the binary using a packer identifier, which is one of the essential tools of malware researchers in analyzing malware. Most good packer identifiers were created for the Windows operating system, so porting a packer identifier to Linux will be discussed. A framework for a packer identifier in Linux that is written in Python will be shown.

BSides Atlanta 2010 PROGRAM

Essential information about packers will be introduced in the presentation, including the differences between packers, file archivers, file binders, compressors, and encryptors; a comparison of packed and unpacked files; and two best practices in identifying packers - signature-based and heuristic-based detection.

Name: Dave Kennedy (@dave_rel1k) and Eric Smith (@infosecmafia)
Title: Strategic Penetration Testing: All Up in Your Shiz
Abstract: The term penetration testing has become one of the many "buzz" words used incorrectly within security policies, regulations and consulting services for a number of years now. Over time the value of the service has been lost partially due to improper testing techniques and methodologies, false expectations, inadequate skillsets, scoping limitations, and most importantly inability to properly relate it back to the business. This presentation will demonstrate some of the more advanced methods of penetration testing to identify the real impact on the target business and provide the necessary value that an organization can understand and act upon.

Name: Chris Nickerson (@indi303)
Title: Top 5 Ways to Steal a Company "Forget root, I want it all!"
Abstract: This will be a highly interactive talk with the audience! The corporate landscape is built on a toothpick pillar and it is time to point it out. This talk will challenge the audience to find flaws in pictures/videos, identify universal weak points in culture and design, as well as go through the top 5 ways to completely take over most of the companies out there. We will blur the line of black/white hat to show how it is done in the real world.

Name: Mike Doyle @fe3mike
Title: Pivoting Arbitrary Tools with Socket Proxy
Abstract: An attack platform can host many tools for reconnaissance, enumeration, vulnerability analysis, and exploitation. These are all too frequently left at the doorstep of the target network once the first host is compromised. Socket Proxy is a post-exploitation pivot tool for leveraging the versatility of your attack platform in the network context of a compromised host.

Name: Gal Shpantzer @Shpantzer
Title: Security Domination via Hard Drive Isolation
Abstract: Every organization is a reluctant participant in the malware arms-race, investing untold blood and treasure in securing the essentially unsecurable: Commercial general-purpose, fat-client endpoints that are simply inappropriate for certain high-risk business processes and sensitive data. This talk goes through this problem and proposes an alternative approach to the one-size-fits-all desktop. SANS.edu grad students call this approach ROBAM, while Gartner calls it Trusted Portable Personality Devices. You will learn how leading government, financial and emergency response sector organizations are improving security while simultaneously extending remote access and mobility to administrators as well as end users. Several specific use-cases are outlined and analyzed in this talk.

TRACK 2: IN THE WATCHTOWER

Name: Gary Palgon @GaryPalgon
Title: A New Approach to Enterprise Data Security: Tokenization
Abstract: To lower the risk of data theft and comply with privacy laws, organizations are seeking ways to secure more types of sensitive and confidential data. A new data security model — tokenization — is proving effective for securing credit card numbers as well as personally identifiable information while reducing scope for PCI audits and lowering business risk across the extended enterprise.

Name: Martin Fisher @armorguy
Title: Why We Suck At Incident Response (and How To Suck Less)
Abstract: If we're honest with ourselves we generally suck at Incident Response. We'll discuss people, process, and tools and reveal the secret to creating teams and techniques that will help us suck less at IR.

Name: Thomas Cross
Title: Unauthorized Internet Wiretapping: Exploiting Lawful Intercept
Abstract: For many years people have been debating whether or not surveillance capabilities should be built into the Internet. Cypherpunks see a future of perfect end to end encryption while telecom companies are hard at work building surveillance interfaces into their networks. Do these lawful intercept interfaces create unnecessary security risks?
This talk will review published architectures for lawful intercept and explain how a number of different technical weaknesses in their design and implementation could be exploited to gain unauthorized access and spy on communications without leaving a trace. The talk will explain how these systems are deployed in practice and how unauthorized access is likely to be obtained in real world scenarios. The talk will also introduce several architectural changes that would improve their resilience to attack if adopted. Finally, we'll consider what all this means for the future of surveillance in the Internet - what are the possible scenarios and what is actually likely to happen over time.

BSides Atlanta 2010 PROGRAM

Name: Tony UV @versprite
Title: Applying Application Threat Modeling Beyond the Conceptual Hype
Abstract: As delusions of effective risk management for application environments continue to spread, companies continue to bleed large amounts of security spending without truly knowing if the amount is warranted, effective, or even elevating security at all. In parallel, hybrid, thought provoking security strategies are moving beyond conceptual ideas to practical applications within ripe environments. Application Threat Modeling is one of those areas where, beyond the hype, provides practical and sensible security strategy that leverages already existing security efforts for an improved threat model of what is lurking in the shadows. This presentation seeks to walk though practical applications and exercises associated with application threat modeling. Integration to multi-security focused disciplines will be included, such as dynamic analysis, static analysis, incident monitoring, vulnerability management, social engineering, penetration testing, and more.

Name: Erik Peterson @silvexis
Title: The Long Con of Automated Dynamic Web Application Security Testing
Abstract: It's been over 10 years since the first automated web security testing products were introduced so why are so many of the dynamic or black box testing tools still challenging to use and often ineffective? With the average organization having hundreds or even thousands of web applications organizations have turned to automated solutions as their only option to assess their online risks, but are automated web application security testing solutions really effective? This session outlines why today's tools and approaches are increasingly only giving us a false sense of security and how a new approach to dynamic web application security testing is required.

Name: Peter Hesse @pmhesse
Title: Security Policies: The Next Generation
Abstract: Today's average corporate information security policy is meant to solve a problem: it codifies practices and rules for dealing with information in storage, transmission, and use. Unfortunately, most policies have become the problem that needs to be solved. With unreadable language, amazing depth, breadth, and length, and unimplementable requirements, current policies only push users further from what they need. This talk will give real-life examples of bad security policy practice, and share a glimpse into my vision of the next generation of security policies which will (hopefully) gain better acceptance and allow for improved awareness.

Name: Mike Rothman / @securityincite
Title: Information Security 2011: Gaze into the Crystal Ball
Abstract: Things seem to be bad out there. More attacks, higher value targets, less budget, declining economy, the list goes on and on. Why do we even bother? And more importantly what can we look forward to in 2011? Will it be more of the same, or is change finally coming to information security? Mike Rothman of Securosis will set the stage for the coming year, discussing the major (and expected) threat vectors. He'll also key trends regarding network, endpoint, and data security. And yes, have no fear, he'll talk about clouds, virtualization, and compliance too. You'll laugh, you'll cry. Actually, you'll mostly cry, but at the end of the session, you should be able to start thinking about your own priorities for 2011.

TRACK 3: IN THE MIX

Name: Logan Kleier @PortlandInfoSec
Title: Is This What the Long March Looks Like: SANS Top 20 Critical Controls Implementation
Abstract: The SANS Top 20 Critical Security Controls are one of several information security guidelines designed to reduce risk and are designed to simplify the process of addressing risk. However, the list is lengthy and requires significant organizational effort to attain basic proficiency in all the 15 automated controls and 5 manual controls. This presentation will help to delineate some methods to prioritize and achieve better success in implementing the SANS Top 20 by understanding the overall organization's motivational and hygiene factors. These motivational factors (first described in psychology literature as the "two factor theory") are factors that drive an organization to do better, while hygiene factors are those factors that cause the organization discomfort when absent but do not cause the organization to do better. The City of Portland has sought to implement SANS Top 20 controls in those areas that align with the City's broader motivational factors and avoid implementing controls that address hygiene factors.

Name: Nick Owen @wikidsystems
Title: Securing Remote Access with Two-factor Authentication & Open Source tools
Abstract: In these times of tight budgets, it pays to explore open-source remote access solutions. This talk discusses how to create robust, secure remote access offerings that are simple and secure. Network protocols, remote desktop, web-applications, VPNs, etc. will be discussed.

BSides Atlanta 2010 PROGRAM

Name: Todd Merrill @ToddMerrill
Title: Protecting PHI with encryption for HIPAA compliance
Abstract: This talk is a rundown of the misery that is the American Recovery and Reinvestment Act and its impact on the Health Care community in the US. The ARRA strengthened the old HIPAA regulations in a number of ways and is now forcing medical practitioners and their Business Associates to finally embrace Healthcare IT, Security and Privacy. Encryption is a vital part of this regulation and will keep you out of trouble if you can implement it properly. http://www.slideshare.net/ToddMerrill/protecting-phi-with-encryption-for-hipaa-compliance

Name: Taylor Banks @taylorbanks
Title: "Letting go of Control: A Twelve-Step Program"
Abstract: Embracing the cloud frequently means relinquishing control of and visibility into certain aspects of your data to third-parties. Regardless of how much or how little you trust those third-parties, it's still possible to protect your data. My name is Taylor, and I am a control freak. This talk will introduce a twelve-step program to help you secure your assets as you let go of control and are assimilated into the cloud.

Name: Brian Wilson @slimjim100
Title: Intro to DOCSIS (how your cable modem works)
Abstract: A quick lesson on how you broadband cable modem gets your data packets from your home to the internet and back over coaxial cable networks. Learn how DOCSIS has evolved from 1.0 to 3.0 and how the CMTS works and controls thousands of modems on a shared network with per modem speeds of over 150Mbs.

Name: Michael Woolfe @wfmn
Title: How to Get Someone Else to do Your Job
Abstract: Working with contractors, under staffed, mergers, remote support, and hiring MSSPs are all scenarios where we have to rely upon someone else to do our job or a job. We'll discuss how to leverage these 'resources' while staying insane, employed, and applying some resemblance of QA.

Name: Daniel Frye @frizille
Title: Basics of Securing PeopleSoft Architectures
Abstract: Many organizations rely upon Oracle's PeopleSoft ERP applications but many organizations treat ERP as 'just another app' to secure and manage. Unfortunately this is not the case and the misconception is opening many organizations to increased risk – especially given the sensitive nature of the data found inside the ERP systems. This talk will discuss "PeopleSoft Basics" as it relates to infrastructure security based on the experiences of running the security team for an ERP hosting provider. The talk will also provide security teams responsible for securing PeopleSoft a starting checklist to validate their own PeopleSoft architectures once they leave the conference.

Name: Karthik Rangarajan @krangarajan
Title: Browser Add-Ons That Steal
Abstract: Both Mozilla Firefox and Google Chrome offer the ability to obtain third party extensions/add-ons to extend functionality. None of these third party add-ons are verified by anyone, except by developers - and that is only in the case of a highly collaborative project. There have been cases where Mozilla has pulled add-ons from the addons site, and has even come up with a plan to code review extensions before they go live. There's already a system in place where addons are scanned for known malware before they are uploaded - but that's only known malware. The code review policy hasn't seen the light of day yet; Extensions that just steal passwords from login forms have been done, and have been taken off. But what if the extension had code that read other things from your computer? Like the database that holds your form's autocomplete. It's not obvious why that is useful - but consider certain websites that don't turn autocomplete off for sensitive information. ATT does that for SSN, Bank of America does that for your account number, there are some sites that do that for your credit card numbers. An extension that could read this information has then given you a mine of data. The usual approach for such an extension is to find an exploit in another one, but if an extension could be pushed in as an innocent one by itself, then it could do a lot more damage.

Name: Daniel Peck @ramblinpeck & Nidhi Shah
Title: Demystifying Web Malware
Abstract: Be it worms, phishing, malware or rogue AV, JavaScript is one of the most common routes for malicious activities. Attackers are using clever obfuscation techniques to deceive AV and combining sophisticated social engineering tactics to take advantage of user ignorance. Whether we're talking webapps, PDF, or flash vulnerabilities, JavaScript cool tricks apply, giving attackers the most bang for their buck. How do these attacks spread, what's behind them, and what do we need to know to mitigate them? This talk will demystify JavaScript malware with an in-depth discussion and demonstration using the latest PDF expl0it, and more.

BSides Atlanta 2010 PROGRAM

SECURITY BSIDES ATLANTA WOULD LIKE TO THANK OUR SPONSORS!

PLATINUM LEVEL

BUILT AROUND YOU sayers

DAMBALLA

WIKID

Sword&Shield ENTERPRISE SECURITY

SecureWorks

ERRATA SECURITY

THINK

BARRACUDA NETWORKS

GOLD LEVEL

mitah apparel

ENDGAME SYSTEMS

nuBRIDGES Sharing Data. With Confidence.

Cloud in 48 Zero to Cloud in 48 Hours!

SILVER LEVEL

STACH&LIU

ISSA METRO ATLANTA CHAPTER

GLOBAL LEVEL

astaro internet security

VerSprite Navigate Beyond Risk

tripwire