DAY 1 - June 10th

Main Hall 0900 - 1030 Nate Cardozo "Opening Keynote Cryptography Law and general Q&A with the EFF"

Nate Cardozo is a Senior Staff Attorney on the Electronic Frontier Foundation's digital civil liberties team. In addition to his focus on free speech and privacy litigation, Nate works on EFF's cryptography policy and the Coders' Rights Project. Nate has projects involving export controls on software, state-sponsored malware, automotive privacy, government transparency, hardware hacking rights, anonymous speech, electronic privacy law reform, Freedom of Information Act litigation, and resisting the expansion of the surveillance state.

Nicollet Room 1030 - 1630 Leonard Jacobs Training - Security 101 boot camp

Security 101 Bootcamp covers some of the cyber security analysis fundamentals that a beginning cyber security analyst should possess

Target Tower 1030 - 1630 Kizz MyAnthia Training - Spy Game: Red Teaming in the real world

During "Spy Game" we will look at the entire methodology of what it takes to execute a successful Red Team engagement. As part of "Spy Game" the attendee will be thrown into the weeds of a real life Red Team scenario.

4th Floor 1030 - 1630 Quick Fire Talks Open Mic

Got something say and need a space? Whether you are a first time speaker or would like a smaller audience to riff with, then Quick Fire Talks are for you. Reserve 15 or 30 minute slots on the whiteboard by the Elevators

Main Hall 1045 - 1130 Tim Crothers "Inside real APT"

We'll delve into comm's resulting from infiltrating C2 (command and control) so attendees can see what "APT" actually looks like and (more importantly) how to detect and deal with them. No smoke and mirrors here. Just the real deal on scumbags p0wning our networks.

Main Hall 1130 - 1300 Lunch and Networking

Main Hall 1300 - 1345 Ty Sbano "Fast Furious and Secure: DevOps Edition"

DevOps and the agile mindset have arrived at large organizations, but security often gets bolted on at the end. This leaves product teams angry and frustrated with security. It is a constant struggle, like Vin Diesel shifting an automatic muscle car. So, how do we ensure that the delivery cycle gets fine-tuned to embed security continuously?

Main Hall 1400 - 1445 Russ Steiger "Maintaining Focus inside the security Maturity Curve"

Lots of companies are building security rapidly, but how will you know what to do next?

Main Hall 1500 - 1545 Paul Melson "Automating Malware Analysis for Proactive Detection"

Analyzing malware can lead to valuable information about adversaries, their capabilities, and intentions. This talk will take a look at practical ways to automate the bulk collection and analysis of malware for the purposes of extracting indicators, developing intelligence, and building detection for new threats.

Main Hall 1600 - 1645 Matt Nelson & Will Schroeder "Bridgeing the Gap: Lessons in Adversarial Tradecraft"

As companies scramble for a way to keep from being the next Sony, they've started to search for ways to simulate the sophisticated attackers they now face. Organizations that have started to adopt an "assume breach" mentality understand that it's not a matter if they're compromised by these advanced adversaries, but when. Red team engagements allow an organization to better exercise their technical, process, and personnel defenses, but much of this advanced tradecraft has been historically restricted to teams with large budgets and timeframes.

Our approach is to help push down some of this advanced tradecraft, so testers can utilize these powerful tactics in assessments of all types. This presentation will cover our view of the "assume breach" mentality, and the approach for our red team operations. We will then trace through several areas where we've made efforts in bringing advanced tradecraft to even constrained engagements. Adversarial tradecraft isn't just for red teams any more.

Main Hall 1700 -1745 Alex Holden "Botnet C&C: up close and personal"

Malware and viruses get more complicated and evasive. Defensive postures concentrate around malware isolation and analysis. But what do hackers see? Taking a page from their playbook we will examine real-life botnet Command and Control systems to see how they function from the inside. Botnet types such as traditional C&C, mobile, RATs, grabbers, injects, and other popular types of hacker tools will be shown to get a better understanding of the hacker back-end platforms and intents for further abuse.

DAY 2 - June 11th

Main Hall 0900 - 0945 Kellman Meghu "The Enforcement Awakens"

There is a new hope for transformation in IT services. Let's explore a cautionary tale about the impact of security in an IoT agile world. What does a secure cloud architecture look like, when you don't have to consider what the product is? Enough with the abstraction layers, you can say it's just computers connected to a network, the impact of the converging technologies are still driving us to change.

Nicollet Room0900 - 1600 Leonard Jacobs Training - Security 101 boot camp

Security 101 Bootcamp covers some of the cyber security analysis fundamentals that a beginning cyber security analyst should possess

Target Tower 0900 - 1130 Kizz MyAnthia Training - Spy Game: Red Teaming in the real world

During "Spy Game" we will look at the entire methodology of what it takes to execute a successful Red Team engagement. As part of "Spy Game" the attendee will be thrown into the weeds of a real life Red Team scenario.

4th floor 0900 - 1345 Anthony J. Stieber Workshop: How to get a job in Information Security

Looking to break into a career in Information Security? Join Anthony J. Stieber, Co-Author of "Breaking into Information Security: Crafting a Custom Career Path to Get the Job You Really Want", as he shows you how to navigate the many pitfalls of joining this profession. Whether you are a student, in IT, security enthusiast, or maybe in Security but looking to climb that next step, Anthony's brings a lot of experience to the table for everyone. Bring your laptops if you have them however they are not required.

Main Hall 1000 - 1045 Jame Renken "Universal Attack Surfaces"

The network is segmented. There's aggressive IDS/IPS all over the place. You've fired everyone who failed your phishing tests, even the CFO. What's left? You're still at risk from the infrastructure you can't control: domain name registrars, SSL/TLS certificate authorities, and even Tier 1 Internet backbones. Seasoned ISP sysadmin James Renken will talk about detecting and defending against social engineering, forgery, and BGP hijacking attacks that we've seen from script kiddies, cybercrime gangs, and nation states.

Main Hall 1100 - 1145 Megan Carney"Micro versus Macro"

Companies that specialize in endpoint security look for patterns across their customer base, then apply those signatures or heuristics to your environment. This is a good thing, even though it often results in false positives. Analysts dedicated to your environment know what's normal and what's not. This is also a good thing. In today's world, you need both perspectives. Modern attackers use camouflage tactics to hide their activity because they're focused on stealing information, for profit or for country. To combat this, you need to combine the macro perspective endpoint security companies give you with the micro perspective your analysts have. This is why you write your own alerts. This presentation will focus on a case study in how Yelp uses intelligence from our DNS resolver to find infected machines, based on deviations from normal patterns in our environment.

Main Hall 1200 -1300 Lunch and Networking

Target Tower 1200 - 1600 Kizz MyAnthia CTF/Red Team Challenge

Not your typical "own the box" CTF, this Red Team Challenge will be team based and challenge your ability as a team to navigate a Red Team engagement. Open to Students of Spy Game Class and all Participants. Lunch will be provided for contestants. Signups will be at registration

Main Hall 1300 - 1345 Nicholas Chapel "Setting up a test lab with VMWARE"

If you aren't fortunate enough to have access to a production environment or on-the-job training, the home test lab is crucial for learning infosec tools and techniques. Creating the testing environment is the first hurdle to overcome in getting hands-on experience, and it can be difficult to know where to start. For those who have not installed VMware before, the prospect may be intimidating, but it is in fact both relatively straightforward and easily taught.

4th Floor 1400 - 1600 Quick Fire Talks Open Mic

Got something say and need a space? Whether you are a first time speaker or would like a smaller audience to riff with, then Quick Fire Talks are for you. Reserve 15 or 30 minute slots on the whiteboard by the Elevators

Main Hall 1400 - 1445 Derek Arnold "Accessible Threat Intelligence with the Splunk app- Optiv Threat Intel"

Optiv Threat Intel is a Splunk App that automatically correlates your data with several popular open threat lists. After a few mouse clicks we can start hunting for log sources that are reaching out to, or being attacked from, known attackers. The app can provide increased visibility to potentially malicious activity going on in the organization.

Main Hall 1500 - 1545 Joe Petroske "Automating Malware Analysis for Proactive Detection"

Image files make great carrier channels for hidden messages. By simply replacing the least-significant bit of each pixel byte with some data, you wind up with an image file with an embedded hidden file. And the new image is indistinguishable from the original. So how could anyone ever detect this? With a

little math and a little Powershell, you can get a good idea whether something else is lurking inside your favorite cat meme.

Main Hall 1610 - 1730 John Strand "If I wake evil (How I would attack you if I turned into a criminal mastermind)"

John Strand is the Owner of Black Hills Information Security (BHIS), and has both consulted and taught hundreds of organizations in the areas of security, regulatory compliance, and penetration testing. John is also an instructor and course author of BlackHat's "Active Defense, Offensive Countermeasures, and Hacking Back" and the SANS Institute's "Hacker Tools, Techniques, Exploits and Incident Handling" classes.

John is co-author of the"" Offensive Countermeasures: The Art of Active Defense" book and is a contributor to the industry shaping Penetration Testing Execution Standard and 20 Critical Controls frameworks."