DEAR PARTICIPANTS

Thank you for joining Security B-Sides MSP 2016!

We've worked hard to bring you the best FREE, community focused, volunteer driven, educational conference. We want everyone to feel welcome and safe so they can engage and discuss our mutual interest computer security and technology.

This year we have three classes, a Red Team challenge led by Kizz MyAnthia, crypto challenges and many prizes!

We, the crew behind BSidesMSP, thank you for joining us at and we hope that you have an excellent time!

Thank you!
Security B-Sides MSP 2016 Volunteers

THE RULES

Be excellent to each other!

Target has provided this terrific facility to us at no cost. We'd like the possibility of coming back in the future. A no cost venue frees up a lot of funds that we can spend on amenities for you instead of venue rental. So please be a good guest.

Policy:

- Be kind and courteous to other attendees, staff and the facility.
- Do not tamper with facilities or equipment.
- Do not access protected physical or logical Target resources.
- Do not try to socially engineer staff.
- Stay within confined areas.
- Do not leave any kind of media behind anywhere.
- Clean up after yourself.

We will have people checking for any illicit activities. We will have off duty cops and security on hand and we will respond accordingly to any such activities. We're going take appropriate actions to ensure the safety of attendees, staff, facilities and equipment.

Help, Information, and Emergencies: Need help or information? Ask registration or staff for any questions you may have. We are here to help! In case of an emergency call 911.
Wristbands: Everyone attending BSidesMSP must wear their wristbands at all times. Photo ID required for admission.
Photography: This event will be recorded and photos taken.
Smoking: This is a no smoking (including e-cig) facility.
Alcohol: No alcohol is permitted at the event.
Firearms: No firearms permitted on premises.

SPONSORS

Target
Black Hills Information Security • 2008 •
RSA
SANS
Check Point SOFTWARE TECHNOLOGIES LTD.
netskope
VERITAS
TITANIA
PRIME THERAPEUTICS
NORSEC
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
AFA ADVANCED FIRST AID, INC.
CRYPTO PARTY MN

BSIDES MSP

Support F Bomb Awareness!

Friday and Saturday
June 10-11, 2016
At Target Plaza Commons
1001 Nicollet Mall, Minneapolis, MN

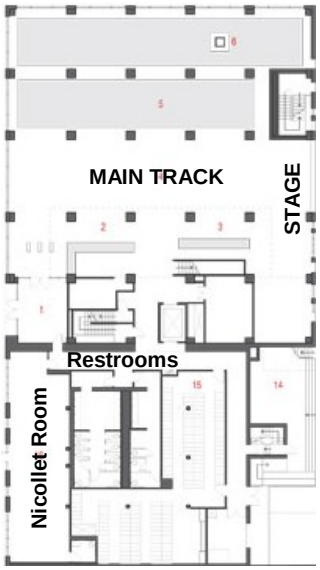
VENUE

Target Plaza Commons
1001 Nicollet Mall, Minneapolis, MN
Nicollet Mall & S. 10th Street Downtown Minneapolis

Doors open: 8am Friday (Join us for coffee!)

Free Bus Transit and METRO Green & Blue Lines
Minneapolis Nice Ride Bike Rack outside the Venue
Parking: One block away in all directions.

FIRST FLOOR



SECOND FLOOR

SCHEDULE

Friday, June 10

TIME	MAIN TRACK LECTURE HALL (1st Floor)	NICOLLET ROOM (1st Floor)	Target Tower (across street)	4th Floor
8am	*Registration Opens*			
8:50 - 9:00	**Opening Remarks**	*Closed*	*Closed*	*Closed*
9:00 - 10:30	**Opening Keynote Cryptography Law and general Q&A with the EFF** *Nate Cardozo*	*Closed*	*Closed*	*Closed*
10:45 - 11:30	**Inside real APT** - *Tim Crothers*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
11:30 - 12:00	**break**	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
12:00 - 13:00	**LUNCH** & Networking	**LUNCH** & Networking	**LUNCH** & Networking	**QuickFire Talk** *Open Mic*
13:00 - 13:45	**Fast Furious and Secure: DevOps Edition** *Ty Sbano*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
14:00 - 14:45	**Maintaining Focus inside the security Maturity Curve** - *Russ Steiger*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
15:00 - 15:45	**Automating Malware Analysis for Proactive Detection** - *Paul Melson*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
16:00 - 16:45	**Bridging the Gap: Lessons in Adversarial Tradecraft** *Matt Nelson/Will Schroeder*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
17:00 - 17:45	**Botnet C&C: up close and personal** - *Alex Holden*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*

Saturday, June 11

TIME	MAIN TRACK LECTURE HALL (1st Floor)	NICOLLET ROOM (1st Floor)	Target Tower (across street)	4th Floor
8am	*Registration Opens*			
8:50 - 9:00	**Opening Remarks**	*Closed*	*Closed*	*Closed*
9:00 - 9:45	**The Enforcement awakens** *Kellman Meghu*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**How to get a job in ITSEC workshop** ***Anthony J. Stieber***
10:00 – 10:45	**Universal Attack Surfaces** *James Renken*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**How to get a job in ITSEC workshop** ***Anthony J. Stieber***
11:00 – 11:45	**Micro versus macro** *Megan Carney*	**Security 101 bootcamp** *Leonard Jacobs*	**Spy Game: Red teaming for the real world** *Kizz Myanthia*	**How to get a job in ITSEC workshop** ***Anthony J. Stieber***
12:00 - 13:00	**LUNCH** & Networking	**LUNCH** & Networking	**CTF/Red Team Challenge** *Kizz Myanthia*	**How to get a job in ITSEC workshop** ***Anthony J. Stieber***
13:00- - 13:45	**Setting up a test lab with vmware** *Nicholas Chapel*	**Security 101 bootcamp** *Leonard Jacobs*	**CTF/Red Team Challenge** *Kizz Myanthia*	**How to get a job in ITSEC workshop** ***Anthony J. Stieber***
14:00 - 14:45	**Accessible Threat Intelligence with Splunk/Optiv threat intel** *Derek Arnold*	**Security 101 bootcamp** *Leonard Jacobs*	**CTF/Red Team Challenge** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
15:00 - 15:45	**Detecting Least Bit Stegonagraphy with Power Shell** *Joe Petroske*	**Security 101 bootcamp** *Leonard Jacobs*	**CTF/Red Team Challenge** *Kizz Myanthia*	**QuickFire Talk** *Open Mic*
16:10 – 17:30	**Closing Keynote: If I wake Evil** *John Strand*	*Closed*	*Closed*	*Closed*
17:30 - 18:00	**Closing Remarks**	*Closed*	*Closed*	*Closed*

PRESENTATIONS

Opening Keynote - Nate Cardozo (Fri. 9-10.30)

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.

Inside Real APT– Tim Crothers (Fri. 10:45-11:30) 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.

Fast Furious and Secure: DevOps Edition – Ty Sbano (Fri 13:00-13:45)

DevOps and the agile mindset have arrived at large organizations, but security often gets bolted on at the end. So, how do we ensure that the delivery cycle gets fine-tuned to embed security continuously?

Maintaining Focus – Russ Steiger (Fri 14-14:45)

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

Automating Malware analysis – Paul Melson (Fri 15-15:45)

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.

Bridging the Gap – Will Schroeder/Matt Nelson (Fri 16-16:45)

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.

Botnet C&C: Up close and personal – Alex Holden (Fri 17-17:45)

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.

The Enforcement Awakens – Kellman Meghu (Sat. 9-9:45)

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?

Universal Attack Surfaces – James Renken (Sat 10-10:45)

Detecting and defending against social engineering, forgery, and BGP hijacking attacks that we've seen from script kiddies, cybercrime gangs, and nation states

Micro versus Macro – Megan Carney (Sat 11-11:45)

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.

Setting up a test lab with vmware – Nicholas Chapel (Sat 13-13:45)

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.

Accessible Threat Intelligence – Derek Arnold (Sat 14-14:45)

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.

Detecting least bit Stego with Powershell – Joe Petroske (Sat 15-15:45)

Image files make great carrier channels for hidden messages. With a little math and a little Powershell, you can get a good idea whether something else is lurking inside your favorite cat meme.

Closing Keynote: If I wake Evil – John Strand (Sat 16:10-17:30)

Whether laid off, replaced by robots, or bored, smart people can do bad things. John explores how he would attack you.

TRAINING & GAMES

Security 101 bootcamp - Leonard Jacobs (Fri 10:30 – Sat 15:30)

Basic Security course for cyber security analysts

Spy Game – Kizz MyAnthia (Fri 10:30 – Sat 11:30):

The course covers real world Red Teaming,

How to get a job in ITSEC – Anthony J. Stieber (Sat 09:00 – Sat 14:00):

If you're new to IT Sec or looking to move up then this workshop is for you. Sign up is 1st come 1st serve

CTF/Redteam challenge – Kizz MyAnthia (Sat 12:00 – Sat 16:00):

RedTeam challenge is open to all, sign up at the event. Space limited to 50.

Crypto Challenge – B-Sides volunteers (Fri – Sat) More info at registration