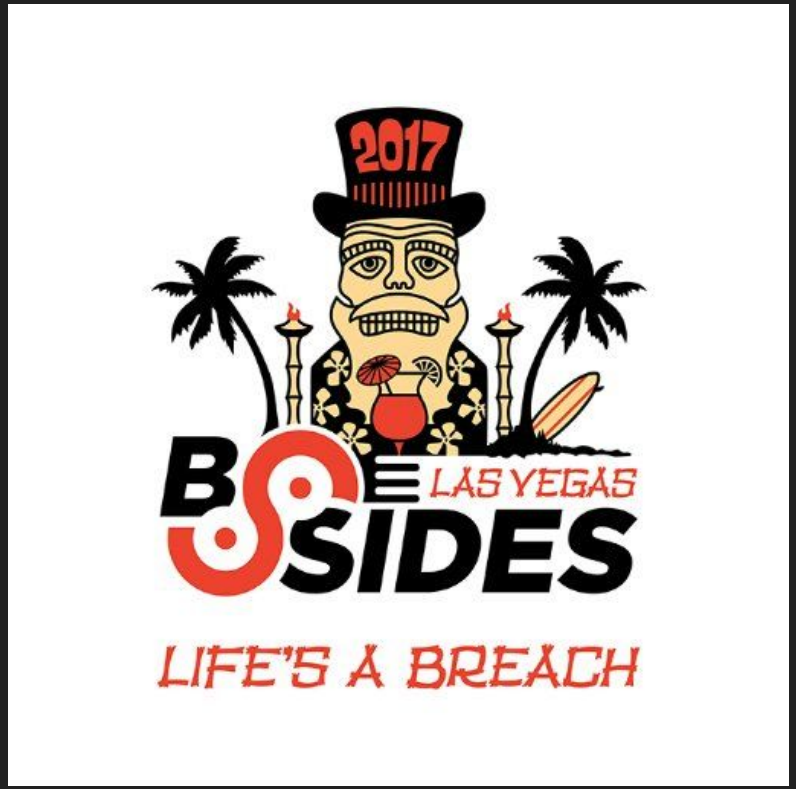
Defcon+Bsides Debrief

Plus other talks

Overview

- BSides Las Vegas
- Defcon 25
- Other Talks

BSides Las Vegas



BSides Tips

- Get there early if your wanting free tickets
  - Staying at Tuscany/Hotel is even smarter
- Head to the hotel the day before at night, there are a bunch of organisers already drinking :)
- The Pool Party is epic fun
- There is a lot of Blackhat Events/Parties, you can also run over to wherever it is
  - TLDR Free Alcohol+Food
- There are so many streams, figure out what you want to see/ what is unrecorded
- Vendor Area: Get in ASAP and steal everything

BSides Streams

- Common Ground
  - General Security
- Breaking Ground
  - New Research
- Ground Truth
  - Data Science
- Hire Ground
  - Career Focused
- I Am The Cavalry
  - Discussions on Infosec (eg Panels and Round Tables)
- Ground1234!
  - Passwords Track
- Proving Ground
  - New Speakers
- Underground
  - NOT RECORDED

Playlist and Videos

- BSLV17_D1_GroundTruth
- https://www.youtube.com/watch?v=xhnjD6AW_Cg&list=PLjpIlpOLoRNSEIRhj-QXn-M10ld9gLjO2
- BSLV17_D2_GroundTruth
- https://www.youtube.com/watch?v=sK_XkBx3cTs&list=PLjpIlpOLoRNQ8ZwXqrIUMLUbi6Qd2rl26
- BSLV17_D1_CommonGround
- https://www.youtube.com/watch?v=mtDsIhzkRNc&list=PLjpIlpOLoRNSaJlHQTxpH4Iy6BefaH4hp
- BSLV17_D2_CommonGround
- https://www.youtube.com/watch?v=CF2RrpzhRuE&list=PLjpIlpOLoRNQxZXPxPUzBkzU5m0iZkPG_
- BSLV17_D1_HireGround
- https://www.youtube.com/watch?v=bfaMaznbhCw&list=PLjpIlpOLoRNQU2TACUTt_NjcjaXqwjiKx
- BSLV17_D2_HireGround
- https://www.youtube.com/watch?v=QpyT5supwZY&list=PLjpIlpOLoRNTgfc8BbgvaMRIgFh8Ypaa2
- BSLV17_D1_Ground1234!
- https://www.youtube.com/watch?v=mmcmKI2CK4g&list=PLjpIlpOLoRNSaex9PzFGIySMBnOhPYT33
- BSLV17_D2_Ground1234!
- https://www.youtube.com/watch?v=CqwbCxP7MC0&list=PLjpIlpOLoRNR5rbe9x-g_ZPeBAUZ_4Eaa
- BSLV17_D2_BreakingGround
- https://www.youtube.com/watch?v=APHIvFaUEKE&list=PLjpIlpOLoRNRf4qID4oeAUvhkSGfWRAnd
- BSLV17_D2_ProvingGround
- https://www.youtube.com/watch?v=rAeuJQrueng&list=PLjpIlpOLoRNSAFQjjU-jpo-WAr9ywOn8G
- BSLV17_D2_I_Am_The_Cavalry
- https://www.youtube.com/watch?v=F095VJ7UReY&list=PLjpIlpOLoRNTU4r_pd0dSYzFBnENGMTvo

Playlist and Videos

However, there are more videos, but they haven't been playlisted by bsides so dont forget to check out the channel!

https://www.youtube.com/channel/UCpNGmljppAJbTIA5Msms1Pw

Recommended Talks

Breaking Ground

BG - The Black Art of Wireless Post-Exploitation: Bypassing Port-Based Access Controls Using Indirect Wireless Pivots - Gabriel Ryan

BG - Microservices And FaaS For Offensive Security - Ryan Baxendale

BG - Writing Malware Without Writing Code - Gal Bitensky

Ground 1234!

G1234! - Protecting Windows Credentials: An Excessive Guide for Security Professionals - Mark Burnett

G1234! - Password Cracking 201: Beyond the Basics - Royce Williams Ground1234!

Recommended Talks - Underground

- Navigating The Alterative Facts of Malware Prevention
  - How To Measure your best vendor
    - Next Gen Antivirus/ Endpoint Management
  - CISCO Talos Came Out ontop
  - You need to measure
    - Cost
    - Vendor Support
    - API
  - Treat it like a research paper; technical debt is REAL
- Skip Tracing For fun and profit
  - Best talk, a 3 letter agent talked about his techniques to track down unsavory types
  - Book: How to Disappear: Erase Your Digital Footprint, Leave False Trails, And Vanish Without A Trace
  - Example:
    - Criminal, bragging and proud of his crimes, caught via MMO
    - Pedo, actually doing skip tracking properly, was desperate for money, baited him into a job app that was made for him

Recommended Talks Underground

- /.git/ing All Your Data
  - Websites leave a /.git directory in root
  - Go find it!
  - https://github.com/securitybites/gittingResponsible
- I Scanned for NSA Compromised Firewalls
  - Looking at Leaked NSA docs and trying to figure out what is epicbanana

Legends


Luke Cusack
@lj_cusack
Following
First in line for @BSidesLV @ 4am
9:06 PM - 25 Jul 2017
3 Retweets 22 Likes

DEFCON 25

AKA I PARTIED TOO HARD AND DIDN'T GET UP EARLY FOR LINECON

Defcon is really big

- 4 Days of Con
- 4 Main Tracks
- 15 Villages (or so)
- Contests
- CTFs
- Scavenger Hunts
- Vendor Area
- Demo Labs
- #badgelife
- MISC MISCHIEF AND ANTICS

Vendors & Swag

- Useful if you haven’t bought stuff in a while
- Lots of wireless and lockpicking gear
- Some books from No Starch press
- Some unofficial defcon mech
- Some vendors

- Swag Area is the where you get official defcon merch

Demo Labs

- Honestly I didn't spend much time here

- https://www.defcon.org/html/defcon-25/dc-25-demolabs.html

CTF, Scavenger Hunts, #badgelife

- Didn’t dive into this year, but there are a lot going on here
  - This is why there are linecon
- https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20ctf/
- https://blog.trailofbits.com/2017/07/30/an-extra-bit-of-analysis-for-clemency/amp/

Talks & Workshops

- Defcon Talks are very slowly coming out as the days go by so keep a look out
- Personally I didnt see any of the main stream talks
  - You will see shortly
- However the slides are up!
  - https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/
  - However, many of them dont make sense without the speaker
  - Some are dual streamed between blackhat/Bsides
- Workshops are up however, and the slides are *amazing*
  - https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20workshops/

Villages (ie where i spent all my time)

- BioHacking Village
  - https://twitter.com/DC_BHV
    - Talks!
- Car Hacking Village
  - http://www.carhackingvillage.com/
- Crypto & Privacy Village
  - https://twitter.com/CryptoVillage
    - Talks!
- Hardware Hacking Village
- IOT Village
  - https://www.iotvillage.org/

- ICS Village
  - https://twitter.com/ics_village
  - http://www.ics-village.rocks/
  - Scada Systems
- Lockpick Village
- Packet Hacking Village
  - https://www.wallofsheep.com/pages/dc25
  - There are also talks!
- Recon Village
  - Talks&Workshops
  - http://reconvillage.org/
  - OSINT
- R00tz
  - Only for kids :)
- Tamper Evident Village

- Voting Machine Hacking Village
- Social Engineer Village
  - Talks&Workshops
- Wireless Village
  - Talks&Workshops
  - http://www.wirelessvillage.ninja/
- 303 Skytalks
  - Where I spent all my time
  - Similar to underground, no recordings
  - https://skytalks.info/

Skytalks Takeaways

- One Click Browswer Defense
  - For people who don't understand computers
    - Ie third world
  - https://blockade.io/
- Advanced DNS Exfil
  - Tool demo
  - https://github.com/ndberry/DNS_Exfil_Tool
  - https://www.nanog.org/sites/default/files/DNS%20Exfil(1).pdf
- Everything you wanted to know about orchestration but were afraid to ask
  - Awesome talk about why the heck we have containers in this day and age
  - Is the coreos dev
  - Continues from last year
  - Pls notes

Skytalk Takeaways

- HUMSEC (or how I learned to hate my phone)
  - Amarok takes us inside his head and makes us question all of our reality
- The Automation and Commoditization of Infosec
  - Two guys get really drunk
  - But this was actually super awesome, all the jobs that have be automated will be
  - Eg, your ‘ssl finding’ pentest report will be automated
  - The only solution is to make this your passion
    - And everyone in this room is already on that path obs
- Robbing the network and ways to get there
  - Tool release portia
  - https://github.com/SpiderLabs/portia

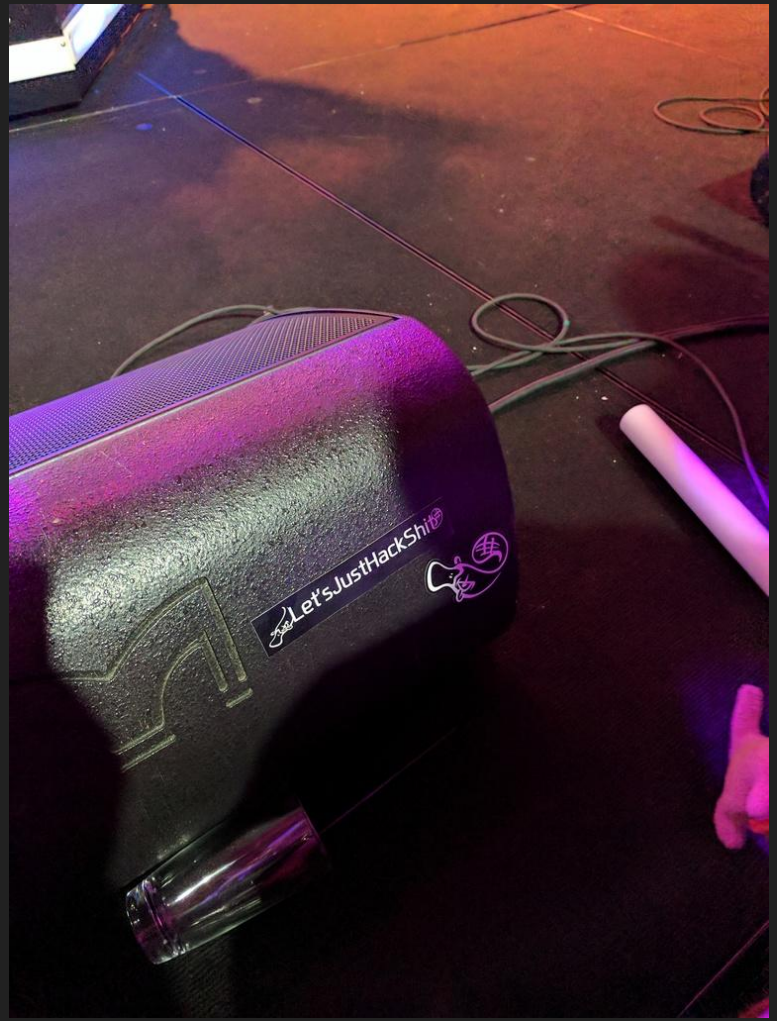
DEFCON PARTIES

- THERE ARE EVEN MORE PARTIES
- BUT YOU'RE PROBABLY PARTIED OUT AT THIS STAGE
- BUT MAYBE GO OUT SATURDAY AS THERE ARE SO MANY PARTIES
- FOMO

- The music and concerts are really fun
- But just talk to people!

BONUS CONTENT

- BSides Manchester Videos Also dropped
  - https://www.youtube.com/channel/UC1mLiimOTqZFK98VwM8Ke4w
- Highlights are the portswigger talks
  - 2017 - DOM Based Angular Sandbox Escapes by Gareth Heyes
    - https://www.youtube.com/watch?v=jlSI5aVTEIg
  - 2017 - Cracking The Lens: Targetting HTTP's Hidden Attack Surface
    - https://www.youtube.com/watch?v=1Newz_wkMvs


Let's Just Hack Shit


THIS IS NOT
A CAMERA

FIN

Also I wish none of you a crying, crawling baby on a redeye flight from SYD -> LAX