Building the DEFCON network, making a sandbox for 10,000 “Hackers”

David Bryan & Luiz Eduardo
Agenda

- David (VideoMan) and Luiz (effffn) Eduardo
- Network history
- Goals
- Challenges
- Network High-Level
- Evolution of the infrastructure
- Wired Network
- Wireless Network
- Future Architecture/Conclusion
David M. N. Bryan

- Computer Security Professional, Aka “Hacker”
- DEFCON network goon
- OWASP Local and National
- DC612 Group
- President of TC Makers Hackerspace
- HAM radio license
- CISSP
- 10+ years security experience
- Play with electronics
- Video, Bikes, Brews beer
- @_videoman_
Luiz Eduardo

- Senior Security Engineer @ NitroSecurity
- Wireless Lead @ DEFCON
- YSTS.org Conference Organizer
- ShmooCon Labs Lead
- @effffn
Network History

- In the beginning... Jeff said let there be internets.
- DC 1 - Sahara
- DC 2 - Sands
- DC 3 - Tropicana
- DC 4 - Monte Carlo, Some interwebs?
- DC 5 - Aladdin, #Fail - maintenance went home for the weekend
- DC 6 - Plaza T1 and ADSL
- DC 7-12 Alexis Park, DSL, T1 from hotel
- DC 13-14 Alexis Park, Wireless PTP high speed (5mpbs)
- DC 15-18 Riviera Hotel - Wireless PTP, 6,12,15,20,100 mbps
Goonage!

David
- Defcon 6-18

Luiz
- Defcon 13-18
Goals

Reliable connectivity
Secure-ish (nothing is completely)
Fast Interwebs

WiFi everywhere there are speakers, events, human networking areas, etc.

Segmentation

• Public
• Speakers
• Press
• Greenroom
• CTF networks
• OpsNet
• Infobooth
• Contests (several)
• Public Servers
• Reg Desk
Challenges

Money
- We have some, but it’s not like it grows on trees

Hotel
- Non-union staff
- Union staff

Infrastructure
- Fiber?

Bandwidth
- Requirements increased each year, mobile video?

Wireless
- Device compatibility
- User density
- Reliability
Challenges

Time
• One week on-site, three days for complete setup.
• We have lots of gear!
• We come from across the country
• Team of 8 people
  • Infrastructure
  • Wifi
  • Video
• Requires logistics & planning before landing...
Network high level

Firewall
- All VLANs end up at the firewall- trunked using port channel
- FreeBSD (was OpenBSD)

Network
- Static routes
- VLANs (~130)
  - 50 DEFCON unsecure Wifi
  - 50 DEFCON 802.1x/Encrypted Wifi
  - 30+ for internal segments

Table of doom
- pre-register to dump network traffic

Wall of sheep
- Everything that is sent over the unencrypted wireless network, and contest VLANs.
Evolution of the infrastructure - DC10
Evolution of the infrastructure - DC12
Evolution of the infrastructure - DC13
Evolution of the infrastructure - DC14
Evolution of the infrastructure - DC14
Wireless Network - Present Day

Riviera Convention Center Floor Plan (Thursday)
Gear Used

Aruba 6000 Controller
AP70 Access Points

• From 18 APs @ DEFCON 14 to 28 APs @ DEFCON 18
• From 4 AMs @ DEFCON 14 to 10 AMs @ DEFCON 18
• (for that matter – from ~500 to ~1000 concurrent users)
• Total Traffic @ DEFCON 18 (wired + wireless)
  Data: 425GB in, 327GB out
WiFi Requirements

- Public Access
- Reliable Service
- Protect the Infrastructure
- (since DEFCON 18) Protect the users
Challenges

- Channel Allocation/ AP placement
- User-density
- Roaming / Mobility
- Minimize “risks” through the infrastructure
- “Deal” with (all types of) attacks
- Device Compatibility
Design Concept

• Centralized Management “goodies”
• (proper) use of VLANs/Subnets
• Block inter-user communication
• WPA2 Encryption + 802.1x Auth
• POE
• “some” WIPS stuff
Future / Conclusion

- New Hotel!!!
- More GBs!!
- 801.11n?
- IDS?
- Logging?
- Lackie?

- www.defconnetworking.org
- DEFCON Photos by EECUE and effffn
Thank you!

David (VideoMan) M. N. Bryan  
Senior Security Consultant  
Penetration Testing, SpiderLabs  
dbryan@trustwave.com

Luiz (effffn) Eduardo  
Senior Security Engineer  
NitroSecurity  
luiz@nitrosecurity.com