



DEFCON 16

- Who am I
 - David Bryan – Aka VideoMan
 - ♦ Hacker, technology enthusiast, security consultant, CISSP
 - ♦ Involved in DEFCON since 1998
 - ♦ Firewall and network design as of DC10 to present
 - ♦ Brews beer
 - ♦ Bikes
 - ♦ Plays with electronics
 - ♦ Works for a Minnesota based security consulting company, NetSPI
 - ♦ dave@drstrangelove.net or david.bryan@netspi.com

www.netspi.com RISK • COMPLIANCE • SECURITY

DEFCON 16

- DEFCON Badge
- TV-B-Gone
- Giveaway!




www.netspi.com RISK • COMPLIANCE • SECURITY

The image shows a yellow DEF CON badge. The badge has the words "DEF" and "CON" in large, bold, black letters. The "O" in "CON" is replaced by a skull and crossbones symbol. The badge is hanging from a red ribbon.

netSPI RISK COMPLIANCE SECURITY

DEFCON 16

- Dan Kaminsky – Man-In-The-Middle DNS Attacks
- Source Port Randomization
- Next Steps
 - DNS SEC
 - D. J. Bernstein hashing



www.netSPI.com RISK • COMPLIANCE • SECURITY

netSPI RISK COMPLIANCE SECURITY

DEFCON 16

- BGP Hi-jacking –
- Peiter "Mudge" Zatkó and Anton "Tony" Kapela
- "Providers can prevent our attack absolutely 100 percent," Kapela said. "They simply don't because it takes work, and to do sufficient filtering to prevent these kinds of attacks on a global scale is cost prohibitive."




www.netSPI.com RISK • COMPLIANCE • SECURITY

netSPI RISK COMPLIANCE SECURITY

DEFCON 16

- The Anatomy of a Subway Hack: Breaking Crypto RFID's and Magstripes of Ticketing Systems
- Massachusetts Bay Transportation Authority TRO




www.netSPI.com RISK • COMPLIANCE • SECURITY

netspi RISK COMPLIANCE SECURITY

DEFCON 16

- Major Malfunction – Feed my Sat Monkey
- <http://www.rfidiot.org>
- http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-major_malfunction.pdf



www.netspi.com RISK • COMPLIANCE • SECURITY

netspi RISK COMPLIANCE SECURITY

DEFCON 16

- Medeco Keys Cloned
- Photocopy
- Xacto-Knife

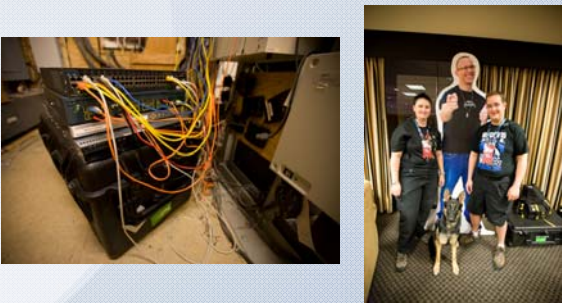


www.netspi.com RISK • COMPLIANCE • SECURITY

netspi RISK COMPLIANCE SECURITY

DEFCON 16

- NOC on Wired Blog
- <http://blog.wired.com/27bstroke6/2008/08/a-first-ever-lo.html>



www.netspi.com RISK • COMPLIANCE • SECURITY

netspi RISK COMPLIANCE SECURITY

DEFCON 16

- VOIP Teaser
 - Record - C
 - Inject - I
 - DOS - A
- Tools Used
 - TrixBox (Asterisk)
 - ettercap
 - rtpinject.py
 - sipp




www.netspi.com RISK • COMPLIANCE • SECURITY

netspi RISK COMPLIANCE SECURITY

DEFCON 16

- Questions?
- Giveaway!



www.netspi.com RISK • COMPLIANCE • SECURITY

netspi RISK COMPLIANCE SECURITY

DEFCON 16 References

- <http://www.dowpara.com>
- http://www.tech.mit.edu/V128/N90/subway/Defcon_Presentation.pdf
- http://www.defcon.org/images/defcon-16/presentations/defcon-16_silsovc_kapela.pdf
- http://blog.wired.com/photos/unclassified/2008/08/26/alex_alfosov_bony_kapela_550x.jpg
- http://blog.wired.com/shared/image.html?photos/unclassified/2008/08/10/defcon_press_conference_18.jpg
- http://blog.wired.com/shared/image.html?photos/unclassified/2008/08/06/kaminsky_by_quinn.jpg
- <http://www.flickr.com/photos/teecue/589702449/>
- <http://blog.wired.com/2/2008/08/06/defcon/index.html>
- <http://www.defcon.org/html/99-defcon-media-archives.html#defc-16>
- <http://blog.wired.com/2/2007/08/jernalmyn-a-12.html>
- <http://www.wired.com/politics/security/news/2007/08/medeox>
- http://blog.makezine.com/MAKE1_PTD899.jpg

www.netspi.com RISK • COMPLIANCE • SECURITY
