DEFCON 20 Conference Report – Steve Holden – sholden@pobox.com – 2012.07.31 (1st draft)

NEWS REVIEWS:

Overviews:	Ninja Tel:	Other Stuff:
• Forbes.com • Wired • PC Magazine • ComputerWorld • News 24 • CNET	• Msn.com • Gigaom.com • Arstechnica	• Malware Testing -- Network World • Gun Safes - The Sun Daily • Huawei Routers#1 • Huawei Routers#2

TRAINING RESOURCES:

- http://www.securityuniversity.net/classes_GI_Bill.php
- http://www.thehackeracademy.com/
- http://www.netsecuritydegree.com/

*** Attending talk in person, other notes are based on slides/material provided by DEFCON DVD or speaker. If you are interested in a presentation and can't find it online, then drop me an email and I'll send you a copy.*

Welcome & Badge Talk [The Dark Tangent, LoST, Jason Scott]**

- Badge is very programmable (couple of games - interaction / crypto challenge)
- Made in the USA
- Developer kit is available
- Can add keyboard, mouse, VGA ports via hardware hacking village
- More info: http://forums.parallax.com/showthread.php?141494-Parallax-Propeller-on-DEF-CON-20-Badge-Start-Here

Making Sense of Static – New Tools for Hacking GPS [Fergus Noble, Colin Beighley]

- NO SLIDES ON DEFCON DVD

Socialized Data: Using Social Media as a Cyber Mule [Thor]**

- how a bad guy can use social media (facebook) for bad things
- spectrograms (deltas) - sign language
- amplitude, time, etc analysis of graphical information into sound
- bad guy is looking to hide his data, communicate undetected, control own channels, channels need to be free, channels should be backed (fault-tolerant)
- bad guy can put all his data on Facebook (Mr. Poon Tang)/text, photos, steganography
- embedded text, gps coordinates, etc in specific audio but also hide in audio that sounds normal
- spectrum graphics can be "inserted" into audio, and then you can see the graphics via standard audio tools
- Facebook does 'recode' your video/audio and will drop spectrum that humans can't hear

Passive Bluetooth Monitoring in Scapy [Ryan Holeman]

- good overview of what bluetooth is
- demo and examples of using scapy (python) tool for attacking bluetooth devices
- hardware recommendation ubertooth
- twitter = @hackgnar

Can You Track Me Now? Government And Corporate Surveillance Of Mobile Geo- Location Data [Christopher Soghoian, Ben Wizner, Catherine Crump, Ashkan Soltani]

- NO SLIDES ON DEFCON DVD

Cortana: Rise of the Automated Red Team [Raphael Mudge]**

- iRC hacker from ~20 years ago (jIRCii)

- Cortana is a scripting language for Armitage (www.advancedpentest.com)
- Armitage (GUI for metasploit - distributed, team focus (client-server))
- some of his current work is being funded by DARPA
- Demo (situational awareness bots / scan and report changes)
- Demo (debugging)
- Demo (Windows GUI activity]
- twitter = @armitagehacker

Shared Values, Shared Responsibility [General Keith B. Alexander, Cybercom/NSA]
- NO SLIDES ON DEFCON DVD
- Lots of news coverage: PC World, etc

Owning One to Rule Them All [Dave Kennedy, Dave Desimone]
- NO SLIDES ON DEFCON DVD

The Art of Cyberwar [Kenneth Geers]
- No slides on Defcon DVD but two white papers are included

Don't Stand So Close To Me: An Analysis of the NFC Attack Surface [Charlie Miller]**
- NFC standards review and capabilities - Linux kernel code looks weak - ISO 14443 (4cm range to pick it up), 13.56-MHz, data rates 105-424 Kbits
- looks like it will be "ubiquitous" (active (p2p) / passive)
- Physical vectors, protocol vectors, application level vectors (good list of tools available)
- When is it on? depends -- if being used, and unlocked then probably exploited
- First step is setting up a hardware capture setup (not as easy as he initially thought) -- cards didn't work, software didn't' work, a lot of iterations
- Next step is do some fuzzing options.
- NFC can be generated to do many things at app level, including sending to a URL
- Fuzzing NFC systems crashes many NFC phones/applications (controlling this will be the next step)
- demo: NFC to shell on Google Android
- demo: NFC to bluetooth file upload on Nokia
- found a bunch of other vulnerabilities related to KOffice
- "where there is a magic, there are security problems"
- more tools coming
- NO SLIDES ON DEFCON DVD
- twitter = @0xcharlie

Drinking From the Caffeine Firehose We Know as Shodan [Viss]
- lists devices found on the internet - webcams (including things webcams are monitoring - HVAC), scada, racks, ups, lighting, security systems, etc
- web interfaces
- default passwords
- twitter = @viss

Network Anti-Reconnaissance [Dan 'AltF4' Petro]
- focus on anti-reconnaissance / secure the network
- not access control/IDS/IDP
- Overview of how-to recon / why is it hard to detect?
- options for detection: honeypots, decoys, haystack (demo tool)
- still have classification issues (log analysis, signatures, etc) that may require doing machine learning (k-nearest neighbor, scalar values)
- twitter = @2600AltF4

How to Hack VMware vCenter Server in 60 Seconds [Alexander Minozhenko]
- fuzzing focused research / outlines test environment
- overview of vCenter / web interfaces (Jetty)
- VASTO metasploit modules

- current vectors: arp poisoning, ssl certificates, directory traversal
- another issue: md5 password files with no salting (vulnerable to rainbow tables)
- some pswds in the clear
- hardening suggestions: latest patches, limit admin services, read the hardening guides
- twitter = @al3xmin

Changing the Security Paradigm: Taking Back Your Network and Bringing Pain to the Adversary [Shawn Henry]**
- former FBI agent, very high-level threat analysis and why computer security is relevant
- NO SLIDES ON DEFCON DVD

Scylla: Because there is no patch for human stupidity [Sergio Valderrama, Carlos Rodriguez]
- Tool for doing password audit testing
- Supports a bunch of protocols and applications
- Nice whitepaper

Crypto and the Cops: the Law of Key Disclosure and Forced Decryption [Marcia Hofmann]
- NO SLIDES ON DEFCON DVD

Attacking the TPM Part 2: A look at the ST19WP18 TPM device [Christopher Tarnovsky]**
- NO SLIDES ON DEFCON DVD
- These chips are used to secure items like Bitlocker
- His research says these products are not that strong
- Zoom (optical) analysis - copying and review bits - ROM is not encrypted

Detecting Reflective Injection [Andrew King]
- this is tool to help defenses
- RID.py
- definition of reflective injection (lazy programmers)
- focus of defense: monitor memory and VirtualAllocEx
- uses white list of what is expected and then starts monitoring
- then validate legitimate pages, and legitimate threads
- once you find something, save to disk and then scan with A/V
- you could once you find this type of issue, then do a reflective injection into their space to screw them up (note A/V will probably alert on this - run-time obfuscation will be needed)

An Inside Look Into Defense Industrial Base (DIB) Technical Security Controls: How Private Industry Protects Our Country's Secrets [James Kirk]
- review of NISP, NISPAC, NISPOM
- C&A process
- Security Controls / STIGs / ISL 2009-01 (Linux, Windows)
- weakness: patches, usb, VM, UAC, non-auditing, tamper

Bypassing Endpoint Security for $20 or Less [Phil Polstra]**
- twitter = @ppolstra
- USB attack vector analysis
- solutions are geared to trying restrict portable media (aka MAC filtering - white list)
- review of the history USB (now v3.0 with 5-Gbps)
- hardware/software is designed to be as simple as possible (12 steps - mostly hidden from the user)
- USB endpoint: 'virtual pipe' + control
- Windows machines will only look at first partition so if you put your data on a different partition plus use a non-standard Windows file system, you could probably hide information pretty well
- File systems: FAT, FAT32, NTFS, etc. [block based]
- On Linux you can turn Wireshark into a bus sniffer
- USB hacking chip options (for building your next project to bypass endpoint protection) - Weak (Ardunio, PIC) Strong (FTDI Vinculum II) [slide deck has complete details]
- basics: VID/PID negotiation (with your project doing impersonation of an approved VID/PID)

- Windows vs. Linux
- Testing (Linux Udev Rules - White List)
- demo (pass through device - set VID/PID - then device works - github software available)

Post-Exploitation Nirvana: Launching OpenDLP Agents over Meterpreter Sessions [Andrew Gavin, Michael Baucom, Charles Smith]
- review of the open source OpenDLP data discovery tool for file systems and databases
- works on Windows, Linux, and multiple DBs
- agent-based architecture (profiles, admin)
- software developed bridges Metasploit and OpenDLP making it possible to send OpenDLP as payload without admin credentials
- allows penetration testers to leverage OpenDLP for data enumeration
- code is available - demo

Life Inside a Skinner Box: Confronting our Future of Automated Law Enforcement [Greg Conti, Lisa Shay, Woodrow Hartzog]
- Why, Mediation, Sensor Ubiquity, etc
- Automation is coming to law enforcement (unattended sensors with algorithms determining if something is criminal)
- If something is criminal, then will punishment also be automatic and automated.
- Sensors (car, phones, medical devices, etc) that LE will have access to
- Facial Recognition, Vehicle Tracking of video (traffic, physical protection, etc)
- Location Tracking
- Baiting / Speed Traps
- Social Media
- Punishment (Taser iRobot) / Confinement (trackers)
- Things we need - ability to resolve false positives, false negatives, misidentified, etc
- Good presentation

DivaShark – Monitor Your Flow [Robert Deaton]
- no slides on Defcon DVD

Safes and Containers – Insecurity Design Excellence [Marc Weber Tobias, Matt Fiddler, Tobias Bluzmanis]
- review current safes and containers
- many gun safes are not secure (easy to bypass)
- current standards are worthless (CA DOJ)
- reviewed 10 safes; listed bypass techniques; all were gotten into per slides

Anti-Forensics (AFF) and Anti-Anti-Forensics (AAF): Attacks and Mitigating Techniques for Digital-Forensic Investigations [Michael Perklin]**
- digital investigation focus
- there are good mitigation options but they make things take longer
- current methodologies: copy first ask questions later; assess relevance first and then copy (key word search); remote access on live system and then copy only targeted evidence (enterprise/PI do this more than legal)
- anti-forensic techniques: scrubbing, encryption, physical destruct
- presentation of a detailed ROI analysis
- AF Technique #1 - Data saturation (many many disks, devices, CDs, DVD, etc) [mitigation = drive duplicators]
- AF Technique #2 - Non-standard RAID with non-standard settings (change controllers also causes issues)
- AF Technique #3 - JPEG file heading example - change header files / masking / tool Transmogrify (mitigation = fuzzy hashing (what % is the same))
- AF Technique #4 NSRL/NIST database of Hashes of known files (dll, exe, pdf, etc) a.k.a De-NISTING (change every file by a bit then everything will match - careful for DEP/Windows - CRC change)
- AF Technique #5 - Histograms (date data) ... scrabble your MAC Times (tool Timestomp - randomize) - change bios time to different times / not the same as real time / disable last access updates in registry
- AF Technique #6 Use DOS file names: CON, PRN, AUX, NUL, COM1, etc [you will get some errors from windows but there are easy ways to do this]
- AF Technique #7 circular references, link to parent to child to parent (nested file searches with slow down investigation)
- AF Technique #8: broken log files (start record bytes inserted throughout the log)

- AF Technique #9 Use lotus notes for email (NSF files are really hard to deal with)
- AF Technique #10 Create Hash Collisions (badfile.doc = goodfile.doc) Very hard to explain especially when hashes are supposed to be unique
- AF Technique #11 Create a dummy hard drive (boot off of USB-key, mimic normal use - news, webpages, sync mail, dummy account) / boot CDs / network analysis can be used for any cloud computing storage)
- AF Technique #12 Make sure that most data needs to be saved through the life of the legal process
- Scott Moulton's DEFCON17 talk is worth watching
- Updated slides at: http://www.perklin.ca/~defcon20/perklin_antiforensics.pdf

The Art of the Con [Paul Wilson]
- no slides on Defcon DVD
- website = http://www.conartist.tv/

Defeating PPTP VPNs and WPA2 Enterprise with MS-CHAPv2 [Moxie Marlinspike, David Hulton, Marsh Ray]
- no slides on Defcon DVD
- Tools mentioned: Cloud Cracker https://www.wpacracker.com & chapcrak

World War 3.0 - Chaos, Control, & The Battle for the Net [Panel]**
- Privacy vs. piracy
- Panel = Joshua Corman, Dan Kaminsky, Jeff Moss, Rod Beckstrom, Michael Joseph Gross
- Anonymous: geo-political change (nation state, individuals, inter-governmental organization, multi-national organization)
- Beckstrom Vision: anyone can talk to anyone they want [Internet most be neutral, local, open, limited regulation]
- Reliability (technology sucks, we have some big problems, alternatives are usually worse)
- Dan Kaminsky "We basically have a system [the Internet] to push pictures about cats."
- TWITTER = @M_J_Grissm, @TheDarkTangent, @JoshCorman, @dakami, @RodBeckstrom

Creating an A1 Security Kernel in the 1980s (Using "Stone Knives and Bear Skins") [Tom Perrine]
- no slides on Defcon DVD
- twitter = @tomperrine

Bruce Schneier Answers Your Questions [Bruce Schneier]**
- Quantum computing threat to public key encryption (not sure what else it can do) - it can have a future impact on specific types of algorithms, but there are currently I/O issues not yet solved
- Can hacking be taught? Domain specifics yes, but the "sideways" look at the world -- he is not so sure.
- Opt Out of TSA Scanner = get a pat down but not a metal detector + pat down (not sure why as that would probably be "more secure")
- Common Criteria / Other standards, are there any options to improve?
- Banking sites really secure? / pretty secure, seems to be working, things could be getting worse though
- Thoughts on how users choose passwords? / users can't pick good passwords - security needs to solve this for them

Owning Bad Guys {And Mafia} With JavaScript Botnets [Chema Alonso, Manu 'The Sur']
- Examine current botnets and determine vulnerability level
- Man in the Middle Scheme = take over command and control signals (ARP spooking, DHCP, ICMP, SLAAC, DNS, etc)
- Man in the Browser - JavaScript is the Middle (inject into it -- example Google analytics JavaScript)
- tools = beefproject.co , tor, squid proxy

Stamp Out Hash Corruption! Crack All The Things [Ryan Reynolds, Jonathan Claudius]
- Slides + WP + Tools available
- twitter = @reynoldsrb
- if you can get the hash, you can do privilege escalation, password analysis, forensic investigations
- review Windows password hashes (LM / NTLM) & how to get them
- cracking via John the Ripper and Rainbow Tables not reliable for injecting back into registry
- good list of registry extraction tools and what is wrong with them today / working on patches

Cryptohaze: Cloud Hacking [@Bitweasil]
- Site = http://www.cryptohaze.com

<GHz or bust!: leveraging the power of the chipcon 1111 (and RFCAT) [Atlas]

- overview and attack vectors related to FCC spectrum <GHz (unlicensed ISM / US / European / Other)
- tons of products in this area
- tool - RFCAT + doggles / SMART RF Studio
- frequency usage by device type (good list)
- summary info on: channels, spacing, bandwidth, encoding, etc.
- update and summary of FHSS
- how to setup a lab and tools
- quick review of smart power meter analysis (needs more focus)

Botnets Die Hard – Owned and Operated [Aditya K. Sood, Richard J. Enbody]**

- twitter = @AdityaKSood
- how bots spread, how they do post exploitation, how they spread via HTTP & browsers
- demos (USB Spreading, Ruskill, DNS Changer, Crypto attacks, web injects, forms)
- conclusion (getting stronger, exploiting browsers, HTTP for data exfil, turning them off is very hard)

The End of the PSTN As You Know It [Jason Ostrom, Karl Feinauer, William Borskey]

- no slides on Defcon DVD

Hardware Backdooring is Practical [Jonathan Brossard]**

- slides + WP on DEFCON DVD
- tool = rakshasa (supported across industry, etc), kon-boot (code available)
- FUD = China has a backdoor into everything
- the real problem is the x86 architecture (1981) / TPM is too low in the architecture so it can be re-routed or ignored
- summary of rootkits and getting control of hardware as soon as possible (significant advancement from 2007 until now)
- Goals of malware/backdoor (persistent, stealth, portable, remote access, remote updates, non-attribution, cross network perimeters, redundancy, evade AV)
- insert in the logistics chain - rootkit (malware), and then create links in iPXE, SealBIOS, COREBOOT back to the rootkit (fetching using HTTPS using network connection)
- Demo: BIOS focus, rotating C&C using standard sites and then do the real CC (hard to shut down), re-apply the 'bad' BIOS on a TPM/Truecrypt/Bitlocker can still get in
- Anti-virus can catch main kon-boot but after running through a 'packer' it will not be seen
- This can also target VMs
- When you get a computer you need to start with re-flashing all devices
- summary - list of how to backdoor like a nation state

Hacking Measured Boot and UEFI [Dan Griffin]**

- This can possibly be a solution to rootkit
- It is still "programmable" does allow: secure boot, measured boot, remote attestation, and TPM
- Windows 8 ARM is going to be fully UEFI (screw te Linux community - but also allows app store validation, protects against security vulnerabilities, helps OEM/ISV, etc)
- good docs at Intel TianoCore with hardware available from Intel and BeagleBoard
- good overview how the process works (work flow, etc) in the slides
- tool = Measured Boot Tool (mbt.codeplex.com)
- weakness = if the user is a bad guy then UEFI will not really offer much protection, tools still developing, hibernate files are unprotected, hardware is still evolving, a lot of complexity on both H/S, key management is going to be a challenge (vendor lists)

Uncovering SAP Vulnerabilities: Reversing and Breaking the Diag Protocol [Martin Gallo]

- overview of the key SAP components and ports / then digs into all the details
- the "Diag" is the key focus of research since 2009
- SAP announces security patches but never details
- findings of research: packet dissection, fuzzing at the network level, found & reported (CVE) vulnerabilities
- outlined some attack vectors
- defense and countermeasure commendations: network restrictions, client encryption (https), patches, more testing (especially audit, change management, penetration, etc)

- blog = http://blog.coresecurity.com/author/martin-gallo/

The Safety Dance – Wardriving the Public Safety Band [Robert Portvliet, Brad Antoniewicz]**
- no slides on Defcon DVD
- twitter = @rportvliet
- blog = http://blog.opensecurityresearch.com/
- coverage of how to use 4.9-GHz (trying to use standard 802.11)
- 5.9-GHz for intelligent transport systems (802.11p) / being used in NY with trucks / expected to be used collision avoidance / driverless vehicles
- searching and tracking signals can be tricky
- sites = radioreference.com, caprad.org, wireless.fcc.gov [sometimes you get very accurate data but not always],
- regional planning committees manage the use of these frequencies
- best device they found Proxim Tsunami 4954 MP 1.1, another was the Ubiquiti 5-GHz NSM5 Airmax World version (not the US version)

DDoS Black and White "Kungfu" Revealed [Anthony 'Darkfloyd' Lai, Tony 'MT'Miu, Kelvin 'Captain' Wong, Alan 'Avenir' Chung]
- Consolidated research on the state of DDOS
- Target #1 = Layer 7 (HTTP) / signature IDS did not see their attack combos from Demo 1-3
- Target #2 = TCP (pretty successful)
- Mitigation = network authentication, HTTP 'interrupts', application gateways, network design on where load balancers go, blacklist/whitelist IPs

Black Ops [Dan Kaminsky]
- no slides on Defcon DVD
- twitter = @dakami

Hacker + Airplanes = No Good Can Come Of This [Renderman]**
- Brad Haines, @ihackedwhat, renderlab.net
- don't try this other than in a lab [EFF vetted presentation] -- see 46308 U.S. Code
- this research started by Planefiner AR (iPhone) in Oct 2010 - GPS, direction, web lookups of flights, etc
- planefinder.net, flightradar24.com, radarvirtuel.com (aggregated data) -- pretty much real time / Google maps, types of planes, etc
- review of current Air Traffic Control system (ADS-B Out/In; GPS)
- Unencrypted and unauthenticated (simple PPM), no validation that the aircraft ID is correct
- ADS-8 will be on all U.S. planes by next 10 years
- You can track non-cooperative flights (Air Force One)
- Untrackable Private Plane tracking (not part of ADS-8)
- What is the effect of "injecting ghost flights", what about injecting into a plane
- GPS jamming (NK, some truck drivers using them, NJ airport interference - dealextreme.com)
- GPS Spoofing (Iranian drone attack on US drone)
- OTHER: Airplanes have a bunch of embedded systems (engines, etc)
- Mitigation: mismatch resolution, tailored arrived (also a big issue but needs more research)
- Nick Foster Demo (GNU radio inject output into a virtual plane program and into the tracking system and could put to planes - real vs fake)
- One more thing - TCAS (collision avoidance) -- they work together with ADB-8 [SPOOFING issue, autopilot corrective action] // assumes everyone is cooperative

Spy vs. Spy: Spying on Mobile Device Spyware [Michael Robinson, Chris Taylor]
- malware is readily available for purchase against android systems
- spyware is also available for blackberry, iPhone, windows mobile, nokia Symbian
- nearly everything can be grabbed off the phone: GPS, SMS, email, browser, logs, SIM, etc
- you can also get interactive and take videos, record audio, wipe the phone, mirror users screen
- exfiltration is usually just the Internet
- demos
- can you figure out if you have spyware? Yes ... with the right forensic tools. Review of evaluated spyware against forensic tools is very detailed.

Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit [Dustin Hoffman, Semon Rezchikov]

- no slides on Defcon DVD
- Twitter = @eigenstate

The Darknet of Things, Building Sensor Networks That Do Your Bidding [Anch, Omega]

- twitter = @boneheadsanon
- Couple of technologies: ZigBee (802.15.4) - low power, many advantages, some limitations; 6LowPan (IPv6)
- Let's build for DEFCON 21 a huge sensor network (not Ardunio - too complicated)
- Next year's badge: hardware reference platform agreed to now (uses peripherals)
- Demo (arm.dcgdark.net)

The DCWG Debriefing – How the FBI Grabbed a Bot and Saved the Internet [Paul Vixie, Andrew Fried]**

- no slides on Defcon DVD
- Operation Ghost Click (DNS Changer to user computers and some Cable/DSL modems) -- just created ad changes so you'd see the bad guys ads -- they also blocked all anti-virus updates
- After their bad servers where taken offline they had to take over an clean the DNS services for the infected systems

SIGINT and Traffic Analysis for the Rest of Us [Sandy Clark, Matt Blaze]**

- twitter = @sa3nder (Clark), @mattblaze
- research from the University of Pennsylvania and funded by the NSF
- evaluation of APCO Project 25 (P25) - two way radios used by security organizations (replaces analog FM systems)
- cryptographic security analysis is part of the r&d [there is a white paper on this]
- review of the voice protocol (freq., data rate, encoding, broadcast, symmetric encryption, keys loaded in advanced, Type1 crypto can be supported)
- there is a re-key option over the air but it not very fancy
- they have found that in encryption mode you can still get very good passive traffic analysis, you can also do some active traffic analysis (ping at will - non transmitting radios)
- Marauder's Map - using a two bases of fixed locations using DF antenna arrays you could find all radios in an area
- DoS -- jamming (14dB less energy) is possible by messing with the error correction codes [review of the jammer they built -- GirlTech IMME instant messenger toy ($15) + external power + antenna]
- Selective DoS - jam only random # of encrypted packets which will make the user to assume that the radio only works in un-encrypted mode
- They also found some usability issues that make it not always clear that encryption is enabled (rekey is also a problem) [also users usually announce in the clear that they just rekeyed]
- ref: Poor Crypto Feedback whitepaper (199)
- Motorola KVL-3000 keyload is very $$ and hard to use
- r&d - SIGINT network built to determine how often (from a scientific perspective) federal traffic ends up in the clear [scenario is a FIS setting this up in an area of interest] - used the Icom R-2500 - findings = occasional sensitive data in the clear but all metadata in the clear [great for traffic analysis - who, what, where, when, how, why]

Trustwave, OPFOR 4Ever [Tim Maletic, Christopher Pogue]

- twitter = @cpbeefcake (Pogue)
- review of the current state of security industry: incident response, forensics, penetration testing (PT)
- OPFOR (training) vs. Red Team (testing)
- Recommendation is to turn current penetration testing efforts to more of an OPFOR model (attack and defend all the same page)
- SNIPER Forensics (dcdrawings.blogspot.com) vs. Shotgun Forensics (old school)
- focus on: how was infiltration happen, what did they do (aggregation) and what did they get out (exfiltration) [Breach Triad]
- Locard's Exchange Principle: deductive reason
- Occam's Razor: the simplest answer is usually right
- The Alexiou Principle: What is your question, what data do you need, how do you analyze the data, what does the data tell you
- Exploits are tracked/rated by CVSS (but we need to fix this as white hat completely uses CVSS)
- Black Hat (bad guy approach): attack library, internal network options, how complex is the overall effort

- New goals for PT: stealth, multi-step attacks, blend methods (external, social, internal), data exfiltration [just getting shell is not the answer]
- Demos

Improving Web Vulnerability Scanning [Dan Zulla]**
- a lot of tools out there, improve the strategy
- current we change 10 tools together but miss CSS Rendering, JS Execution, Image Rendering, etc. [sometimes a black box approach]
- Looking to build something that is more reliable
- Current tool review: skipfish (not good for JS but great for straight HTTP); w3af (python HTML tool); sqlmap (great for SQL injection)
- current approach -- python scanner that sits on top of webkit (QWebKit, Pyside) > can get into flash, JavaScript, and other dynamic options
- demos/examples
- fingerprinting web authentication (2 visible fields, near each other (1px to 20px), parallel)

Post Metasploitation: Improving Accuracy and Efficiency in Post Exploitation Using the Metasploit Framework [egypt]
- no slides on Defcon DVD
- twitter = @egyp7

Owning the Network: Adventures in Router Rootkits [Michael Coppola]
- no slides on Defcon DVD
- twitter = @mncoppola
- more info at = http://poppopret.org
- .npk packages on mikrotik router (socks proxy, vpn, IPv6, KEM/KVM virtualization) >>> can we get shell?
- ref = OpenWRT/DD-WRT, firmware-mod-kit, devttys0.com
- targets = NETGEAR WNR1000v3, WGR614v9, FD57230-4 v1110, TEW-652BRP v3.2R
- approach = get image, analyze the image, insert payload, repack the image, load
- test lab problem -- need to hook up an RS-232 serial port to deal with bad payload testing
- from serial port you can setup the TFTP service to get images via Ethernet
- binary blog analysis: boot loader, kernel, file system
- solution was a tool called binwalk (devttys0.com)
- one approach was to replace the call to HTTP and replace it with "bad guy code" and then call HTTP (however this creates an easy to find signature - not a true rootkit)
- Code = to be posted soon, tool is out now, takes image + payload and then you get a new firmware image

Hacking [redacted] Routers [FX, Greg]
- no slides on Defcon DVD
- twitter = @41414141 (FX); @teh_gerg
- [redacted] = Huawei
- Review of the company Huawei
- The NE, AR , CX devices -- "Quidway"
- There is no open security group / no single security advisories / updates don't say what is fixed / not on securityfocus.com / OSVDB
- There OS is a Versatile Routing Platform (VRP) ... the took some things from Cisco IOS (CLI) but not much else -- reality is really VxWorks based
- in the UK they have a copy GCHQ-VRP that is "SECURE"
- how do get in: CLI (SSH, Telnet, Console), Web interface, NETCONF (RPX/XML), SNMP
- debug is only in Chinese
- updates uses BIMS
- there are a bunch of hidden command mode "_"
- VRP images are very hard to get (no legal way) -- so they ended up buying routers, and then pulled the images off the hardware
- image format analysis (headers, binary file)
- default services: SSH, HTTP, FTP, Telnet, X.25, H.323
- BIMS (mgmt. client uses DHCP)

- Code quality analysis - printf # are very high, SSH server is a re-write, OPENSSH fails, NULL-page is executable
- WEB UI is all Chinese; with UID easily guessed, so someone who is already logged in can then run a script and take over that session
- HTTP server UID test/validation appears to be totally buffer overflow exploitable
- example of a shellcode (similar to 2007 Cisco exploits)
- examination of HEAP vulnerability looking at the BIMS clients (the first read by the HTTP read code is vulnerable based on send more data than expected) ... detailed analysis ... demo

Weaponizing the Windows API with Metasploit's Railgun [David 'thelightcosine' Maloney]
- twitter = @thelightcosine
- Current Windows Meterpreter: straight access to Windows via process memory inject for CMD shell and supports post-exploitation
- Railgun is an extension to Meterpreter that allows for loading any known path DLL (this enable dynamic access to a windows system as any user)
- Overview on how it works: LoadLibrary, GetProcAddress, Memread, Memwrite
- Reason to use this: All Windows API available without increasing the size of the payload
- Examples: decrypt third party passwords on the system, capture and decrypt RDP passwords, scan for wireless devices, list all domain controllers, etc
- Demo

SQL Injection to MIPS Overflows: Rooting SOHO Routers [Zachary Cutlip]
- twitter = @zcutlip
- there is a companion whitepaper (wp)
- target: Netgear WnDR3700 v3 (fancy, DLNA, file server via USB)
- for testing -- hook up internal USB port for debugging
- focus of attack (DLNA - Digital Living Network Alliance that enable multimedia between devices)
- DLNA source code is open source
- Able to insert into SQL DB that offers user music library services
- then worked on using SQL inject to pull passwords (success)
- Also able to get root cmd (more difficult but demo'd)

Pwned in 60 Seconds: From Network Guest to Windows Domain Admin [Zack Fasel]**
- twitter = @zfasel
- NTLM Relay, new tool to do cross protocol relay, get windows to auto-auth
- refresher on NTLM (password storage/network authentication) / hash (LM is bad/weak and NTLM is stronger but still has some problems) "pass the hash" issues (still need privilege account not guest)
- NTLM (Version 1/2/3 with Type 1, 2, 3 msgs) client-server comms
- Windows Integrated Auth (http, trusted zones, SMB)
- Guest and NTLM Relaying -> Rogue server -> send to main target (but this has been around for a long time 1999, 2001, etc) < patched in MS08-068 in 2008 >
- 2010 (SSL not being used) - Fire Sheep (user impersonation)
- Could a version of Fire Sheep be written for NTLM
- 2012 (Black Hat, fake talk msg, rejected DEFCON) - restarted tool
- TOOL = HTTP/SMB Rogue Server, Rules for Execution, Automated Execution (ZACKATTACK)
- How do an HTML page for SMB Auths >> Playlist wit UNC network path (iTunes/QuickTime)
- <img src = "\\network share"> / all .doc files (or other Microsoft files) will do the same thing
- Enum User/Groups > latest version of Metasploit (relaying to Domain Controller is hard / LDAP though is available)
- Exchange web Services (external facing) -- NTLM relaying with user names (pull all info from Exchange Web Services)
- Demo (Partial Fail) -- rogue server gets clients/users to connect, can pull their Exchange, SharePoint, etc.
- Solution = switch to Kerberos (then NTLM has to be off)
- Code: zfasel.com/tools

How to Hack All the Transport Networks of a Country [Alberto Garcia Illera]**
- no slides on Defcon DVD
- focus on subway systems, train kiosks
- some of these devices in the "system" (kiosks) have touch interfaces, can do some web stuff, projections, filter, etc
- kiosk system gave access to print dialog box, and you can drop into System 32

- could also FTP client is with browser / nothing really great on them
- machines can see the router ... with a ping app (pingeador) ... with a config file that had a SQL Server connection string -- linked to outside world to get the train stats (history, timing, etc) // very vulnerable // then all the machines disappeared
- free subway tickets (prices and sectors) -- monthly pass (couple of key parts: # string, barcode (CODE_128), sector), changing char+, fuzzing printing of barcode -- created a HACKER ticket for all sectors (but the color was wrong) -- moved the magnetic strip to the "old' right color ticket
- New system is RFID based (staff is also using the same RFID) can you clone the staff one? Yes you can.
- Security Cameras -- all over ... AP network (using WEP and ESSID hidden) ... also not well physical security ... easy to get in and find a good IP ... basically did a IP range and port scan ... SPC Siemens hardware all the security cameras plus door controls ... now do a man-in-middle-attacks with bad certificates
- Train machines (upgrade your ticket, change, etc) ... basic UI ends up getting into IE ... you can cause it to crash and then get to the full windows interface (lots of custom applications -- set up remote access) ... tried HTTP/FTP/HTTPS ... TFTP was there, didn't work but then allowed UDP to right port (strict firewall rules) ... RAT using DNS tunneling ... able to get all the credit card (CC) info stored in log on the system (unencrypted)