DEFCON 19 {DRAFT} Notes

POC: Steve Holden, *personal email*: sholden@pobox.com, phone: 619-631-4433

Version: 1b-personal

Overview: These are my notes {draft} from DEFCON 19. The opinions and assessments outlined below are my own. If something needs to be clarified or supplemented, then please send me email or give me a call to clear any issues up. I listed all the sessions here that I either attended or wanted to attend. If I didn't attend the session, I did review the available slides and added them to my reference folder. If there is a presentation that looks interesting then please let me know and I'll forward on the file that I have for that presentation.

Cybercom (Chris Clearly, no presentation on DVD):

- Good overview of the nature of well-planned attack
- Good details on the military planning process
- Slides sent via email

Amateur Radio (overview) [Krick, presentation on DVD]

- Capabilities (when compared to latest smart phones): Voice, Video Chat, Text Messages, Location awareness, Internet Access. However, missing the app store (most software is however free, shareware, affordable)
- Early handsets that were good: Alinco DJ-580 (first radio) Kenwood TH-77a (best one he ever had)
- Not FRS, GMRS, MURS (not CB)
- ARRL is the legal group (similar to the NRA)
- Narrow bandwidth = longer distance
- Good chart on estimated ranges by 5W, 50-100W, 1500W
- Types: Technician, General, Extra (no Morse code)
- Something to consider (personally) for communicating in a natural disaster or major terrorist attack that takes out significant local infrastructure

SNEAKY PDF [no slides on the DVD]

- Mahmud AB RHMAN @yomuds, Malaysia CERT
- obfuscation within a PDF document
- what do you obfuscate exploit / shell code (give you stealth and make analysis harder)
- need to get around AV and other tools
- good intro on PDF structure (version, components, cross references, trailer, end of file
- components is where: objects, streams, JavaScript, etc. are stored (main focus for most PDF exploits today because there are a lot of places to hide)
- abuse vectors: JavaScript, pdf syntax, pdf implementations
- JavaScript – build the operation, turn it into ASCII, add encoders (Base64 or ROT13) {also good idea to build code in a spaghetti fashion)
- JavaScript Analysis tools: FileInsight, SpiderMonkey, Rhino, V8 (pyV8), jsbeautifer, read in IDE
- Syntax attack (building parsers based on Adobe docs): you can read at beginning of file or at EOF, but you can also start at EOF but you can also have multiple EOF
- PDF features: filter (make the file smaller – hide your stuff in there)
- PDF features: encryption (can hide the exploit but then run when pswd submitted)

- Rich media: shockwave, flash, QuickTime, etc.
- PDF Tools: PDFStream + PDF Examiner

From Printer To Pwnd (Heiland, presentation on DVD):

- PRADEA (www.foofus.net) automated tool for looking at printers, scanners, etc.
- Default URLs are published by vendor and are easy to look up and then see what happens
- Username/Password protections are relatively weak

UPnP-Mapping (Garcia, slides on DVD):

- Overview of the main problems: no authentication, take WAN requests, poor logging
- Review of devices tested for issues (includes standard home routers)
- How the UPnp Protocol v1.0 works / Umap
- Demo SOCKS proxy mode
- Demo Internal LAN scanning
- Demo Manual port mapping
- Mitigation: turn off UPnP to WAN and consider turning UPnP

Black Ops of TCP/IP 2011 (Kaminsky, no slides):

- There are still major protocol and service issues on the Internet
- PNP and other “intranet” technologies continue to leak to the Internet
- Need to find a link to the slides

I'm Your MAC(b) Daddy (Lenik, slides on DVD):

- File system metadata threat vector
- Stored in Master File Table (MFT)
- Can be a good tool for forensic analysis
- Tools: several options are in the slides (log2timeline, regtime.pl)

Three Generations of DoS Attacks (Bowne, slides on DVD):

- review of current open source attacks and problems
- #1.) focus on Layer 4 (take all the bandwidth) – Low Orbit Ion Canon
- #2.) focus on Layer 7 (take out the service) – HTTP tool overview
- #3.) focus on Ipv6: Router Advertisements
- Review: Defending Websites (Mod Security, Akamai cache, Load Balancer, Cloud Flare)
- Slides have a good review of links

Former Keynotes – Round-table Discussion (Sager-NSA, Wells-DOD, DarkTangent, Business POC?!?)

- First NSA released recommendations for security configurations (2001)
- it takes a lot to move the government
- Government (Federal / Military) wants to work with those at DEFCON
- need to continue to work together (people, partnership, etc.)
- Cyber is the new buzz word for IO, CNO, etc.
- the right info to solve the IA problem is out there but not available (Sager)
- Look over the horizon (call over, sensor, etc.) for IA?

- Completing the mission with a focus on people: Navy builds boats and considers what will happen when water gets in (this should be done for IT also) – real people are going to have to do this work [protect us from USB threats, etc.]
- Underground inventory of exploits? Impact for the future? Threat profiles are changing (Anonymous, Lulsec, etc.)

Covert Post Exploitation Forensics with Metasploit (McGrew, Slides, demo files, and White paper on DVD):

- Focus of the presentation is that penetration testers should be more familiar with current forensic tools and capabilities
- Not all forensics need to be done with the physical hardware, a lot can be accomplished remotely
- Topics: File System, Network Remote Access
- Tools: Railgun (run any Windows API or access any DLL via Metasploit)
- Demos

Hacking Your Victims Over Power Lines (Kennedy, slides on DVD):

- Teensy based ('fake' hardware keyboard gear – many variations)
- they were able to get it to type hex and execute via PowerShell (part of Vista, Win7, Win server)
- need to research: shellcodeexec
- power systems over broadband (X10, Z-Wave, etc.) do a great deal of automation and security services (motion, cameras, etc.)
- these things do little in the way of encryption
- Demo of: power line control sniffer and jammer
- Going to be included Social-Engineering Toolkit v2.0

Key Impressioning (Weyers, slides on DVD):

- an approach to lock picking based on periodic but regular access with only short periods of time
- slides are good to understand the approach
- good links at the end of the presentation

Are You In Yet? (Shrdlu, former CISO, no slides)

- Penetration Testing (guns a blazing {single event} vs. horizontal-assessment {comprehensive})
- Tell me (as CISO) what I don't know, I don't want a vulnerability tool scan (I can order that myself and cheaper from another source) when I ask for a penetration test
- Port Flashing is something that causes penetration testers big issues (can be fund for IT to do against attackers)
- Auditors don't talk probabilities (risk analysis), so reports should be tailored to the customer's needs (findings in the report that are “duh”, or cause more unattended problems)
- IT does things on purpose, you (penetration tester) might not like them, but there are business reasons that cause those architectural decisions that aren't always the most secure

Gone in 60 Minutes (Gavin, andrew.opendlp@gmail.com, slides on DVD):

- OpenDLP (data discovery tool web and agent based – LAMP / good for compliance, network/system admin
- Run the tool as after you have root and then grap everything

- Agent gets deployed by SMB, and runs on the Windows box as a “low” priority
- Agent then gets files (uses whitelist/blacklist), search files by regular expression, and then publishes to the SSL web server
- Agent leaves nothing on the system other than log entries
- You do need to plan for a good server (4 cores + a lot of storage)
- Traffic levels are relatively low
- It can use SMBHash for Domain authentication
- DO not install into a folder where you have stuff (c://windows) because it will be deleted on exit
- Good demo
- New version: targets databases, Linux, and additional Windows clients/shares
- Future: Outlook (pst)
- Data is stored on the web server using mySQL (secure data with Trucrypt)

Bosses love Excel, Hackers too (Alonso & Garrido, Slides on DVD):

- informatica64.com / @chemaalonso
- foca – website scanner – v3.0 will be released soon {more research]
- Remote applications (Citrix, Windows Terminal Services)
- ext:rdp in Google (2000 accessible) plus site:gov // you can us BING!
- The configuration files have a lot of information that can be used / bad conf files can be use to generate error messages for fingerprinting
- CACA (Computer Analysis for Citrix Applications) – enumerates a CITRIX server and will tell what worked and didn't
- Windows Server (example with Windows Server 8) gives you too much help / list to help gives you links, shortcuts, etc.
- Live demo using CITRIX demo server on Internet
- Launch Excel %userprofile%
- Shortcut to cmd / PowerShell
- Excel is a very powerful tool
- based on VBA (needed)
- Security Alerts will happen / but users will click them
- Process List
- Get to the cmd.exe, WMI, PowerShell, jscript, cscript, backup directory
- dll injector into Excel to get cmd.exe to run (even if restricted)
- Disable VBA will remove it for all Microsoft products
- No macros (Excel setting) / trusted locations are still enabled / user profile area (client/server) – all policies will disappear (you can removed all trusted locations also in policy)
- Try “only signed-micros” (self-signed will work) – you can then trust the authority and then enable the content / trust all documents [Rogue CA]

Epic Fails of Gun Safes (Deviant Ollam, presentation on DVD)

- Very good presentation and live demo
- Recommend reviewing the slides if you own firearms and expect them to be secure in your gun safe

DIY Non-Destructive Entry (Schuyler Town, no presentation)

- Not able to attend / are there slides?

Smartfuzzing the Web: Carpe Vestra Foramina (Hamiel, presentation on DVD)

- review current testing tool (QA, Testing, etc)
- Tool: RAFT
- current problems: session/state issues, complicated applications, CSRF tokens, stateless via state, proxy, commercial scanners, current requests vs. previous requests
- HTML/Webserver header/browser type
- Login vs. Sign Out (HTML confusion) – confirmation issues also a problem
- Manual testing doesn't script (winmeal? Selinim? - test tools now used for penetration testing)
- Nikto, DirBuster are penetration tools that are now out of date
- RAFT (includes word lists that are from robots.txt)
- What is needed (session mgmt., sequence building, content discovery)
- Response Analysis and Further Testing (RAFT): workflow focus, built-in browser (webkit), no proxy , open source (Python & QT)
- Demo (GET request – request, response, scripts, comments, links, forms, render, generated source, notes)
- Some GUI issues in the most recent version; does include search engine
- Data is stored in SQL-Light
- You can also use the tool to send data back into the service plus DOM functions, crawler, encoder, scripting, cookies, log, etc.
- Traps of Gold (Wilson, presentation on DVD)
- let's be more active and actual consider attacking back people who attacking you
- legal issues for sure but technically is possible (the presentation is about this)
- demos (Metasploit reverse, other tool reverse attack – shell on the offending system using known vulnerabilities)
- Note: for some of the penetration testing tool that are “running a browser” they might not be running it in the standard GUI way so GUI attacks probably won't work

Hacking Google Chrome OS (Osborn, presentation on DVD)

- @mattjay, @theKos (both at whitehatsec.com)
- CR-48 Beta laptop // they are out in production Samsung
- Just a browser – Chrome
- Extensions / Application Store (nothing is stored locally)
- Example: CookieStealer (relatively bad)
- Security attack vector: JavaScript, HTML5, XSS
- Demo: Malicious Extension (Google Voice – page/txt msg, make a call // execute JavaScript // add in memory keylogger for all open tabs/windows // grab LastPass database // conduct XHR scan local subnet looking for items running on Port 80)
- The extensions for Chrome OS are really mini-browsers
- Example: Scratchpad (pre-installed) – automatically syncs to Google Docs; sharing can be enabled by ScratchPad and turn off notifications – JavaScript injected via title of a notes in Google docs / shared to the victim (email notification off), launched via mouse over event and then it pulled down your contacts (cvs), tab.executescript [fixed]

- permissions to what can be talked to (links, sites) is set via whitelist/blacklist or * (all)
- Good overview of Google Chrome API (bookmarks, cookies, history, windows,, tabs)
- Demo of grab LastPass database (very good)
- Some other demo using BeEF (hook'd in via extension and then you get execute_tab, inject_beef, grab_google_contacts, port_scan, send_gvoice_sms)
- The problem of "extension trust" is still the issue that needs to be resolved
- This effects the Chrome browser (which looks like an extension with malicious intent can get to the local file system)

Security When Nano Seconds Count (Arlen, presentation on DVD)

- Focus is the need for as fast as possible transaction processing for Wall Street
- Security is being ignored so that transactions happen faster
- Can they really deploy security in this type environment?

Federation and Empire (Bouillion, presentation on DVD):

- Author of the book "Federation and Empire"
- Outline: Intro, Key concepts, SAML, Identity, WS-Security model, XML, certificates, X.509,
- Demo
- Good list of references and additional information at the end of the slides

Weaponing Cyber Psychology (Sumner):

- Slides be released after DEFCON
- Need to find the link

Web Application Analysis With Owasp Hatkit (Swende, presentation on DVD):

- Testing web applications is typically very complicated
- Good review of proxy testing options
- Tool: HatkitProject (HTTP Analysis Toolkit): proxy, data fiddler, traffic analysis
- Demo

Hacking .NET Applications (McCoy, presentation on DVD):

- Jon McCoy (www.digitalbodyguard.com)
- example: GRAYDRAGON (targets .NET) <injector> / C++ (DLL) / .NET (DLL) enable you to deal with threads // attack via PowerShell via USB << add GRAYDRAGON >>
- You can also use GRAYDRAGON with Metasploit / GRAYWOLF is a decompiler
- You should be admin already to deploy GRAYDRAGON
- Once you do this, any .NET application can be modified (like UNLOCK for a key code)
- This is basically all done after all OS/Application Security Models
- Other code is available: BruteForce (password cracker)
- Demo of GRAYWOLF (decompiler) – only invalid passwords work / find logic areas & decision points and make changes // KeyGens / Cracks for software [Change Key, Call Server, Demo = False, Complex Math
- Demo of changing a Malware Keylogger (finds the code for the password, changes the code to show the password and then put TRUE on the stack so you have the password plus you are in the application)

- Source code / binaries on disk / Obfuscation [time sync but still does not stop understanding what is available] – crypto of code (only unpacked in memory) // “Show Code Base” (playing games – kept as .NET)

Bulletproofing The Cloud (Gomez, presentation on DVD):

- Good overview on the vulnerabilities of “the cloud”: provider, client
- How is it working: Amazon, Rackspace, Softlayer,
- What “clients” should do? – netflow analyzer, IDS, NAC, misconfiguration detection, log consolidation, even correlation
- Tools: alienvault, nfdump, snort, packetfence, syslog-ng, medusa, Metasploit, nmap, simple-evcorr.sourceforge.net
- Demo

Get off of my Cloud (Feinstein, presentation on DVD):

- Review of what Amazon offers (accounts, certifications, identification, etc)
- How users misconfigure Amazon
- How to find “bad” hosted instances/services on Amazon
- TOOL: AMIexposed

Password Cracking GPU (Imhoff, presentation on DVD):

- Chris R attended:
- 8 character passwords can be broken in seconds
- 12+ character passwords are still in the years for cracking
- what are good long password strategies?

Abusing HTML5 (Chow, presentation and some examples on DVD):

- mchow@cs.tufts.edu
- HTML5 = HTML, CSS, JavaScript // still a work in progress
- www.html5test.com
- browsers: Chrome, Firefox, Opera, IE, safari
- Lots of new and some loss functions (see slide)
- All styling of “text” will be done via CSS
- gone: <applet> <frame> <marquee> <bgsound> :-)
- demos: video capture/geolocation {track locations - JSON}
- danager: client-side browser (offline storage (move to 5-GBs), cookies (4KB), session, local db, javascript, cross document messaging, background computation (webworkers – threads)
- All XSS vulnerabilities will be available in localStorage
- WebSQL = Google Gears // so SQL injection will come to the browser
- Other tool: Firebug
- The database feature is there because of “off -line” feature requests
- Application Cache (up to 5-MB) – reduces server loads
- worker.js (webworking) = can create background process with the ability to get messages back
- HTML5 is one way of writing a single application for iOS and Android [growing area of focus]

Metasploit vSploit Modules (Carey, presentation on DVD):

- Good overview of history of Metasploit: architecture, modules, how to use for training vice real world penetration tests
- The vSploit Modules: testing/training focused, can be used stand alone
- Use them for network traffic analysis, device analysis
- Review of the Lockheed Martin Kill Chain concept paper / proposed how vSploit can be used in this scenario
- Demo / Examples
- How to write them via Ruby, Python (pointers to more info in the slides)

Sounds Like Botnet (Kotler, presentation on DVD):

- A look at how VoIP/SIP works and how it is similar in many ways to a BOTNET
- Can it be used for data exfiltration? Yes and other things.
- TOOL: Moshi Moshi
- TOOL: Asterisk

Current Security Threats and Trends (Howard, presentation on DVD):

- Good run down of recent news and impacts
- Presentation provides analysis to predict when some tech becomes mainstream and what threats are going to have mainstream solutions

Cyber-Attack Mitigation Strategies (Geers, presentation on DVD):

- Overview of cyber from a National Security perspective
- Research areas outlined in the talk: IPv6, “Art of War”, Deterrence, Arms Control

Online Scans in China (Zhu, presentation on DVD):

- Joey Zhu (Trend Micro) // Script Analysis Engine
- What the difference between China vs. other parts of the world (PhishTank)
- 1.3 billion people in the country with 0.5 billion online people with 600 million on their top “Facebook” application called QQ
- 100+ sites focused on QQ per day
- Demo: things that seem to work: newsworthy phishing event (focus loss of financial data)
- Bank of China www.boc.com became www.bocxx.com (and also provided RSA token-like input option) // 60 second window for exploitation to occur // cellphone token will have the same issue
- Three categories: Traditional (buy X for Y – huge discount; or money driven link $), Fraudulent (fake site, offering something that is very attractive – plane tickets for 90% off), Scam (Lottery) – pretend to be qq.com or cctv.com [these are looking like 70% of current spam
- spearfishing is not just email but also IM since this is very popular in China
- Security and Stock company scams linked to membership fees
- Target Brand (using Adwords) – ticket flight based on traveling specific popular time or locations (New Year)
- AliPay = PayPal (did $70 billion in 2010) – most Chinese banks support AliPay – bad seller will “fake” denied the purchase, ask you to submit again, $1 will be charged, then they will continue to say your banking credentials are wrong, then please update all your information (which is then stolen)
- You can get a fully working phishing site (code, etc) for $150

- Stories from real world penetration tests (Havelt, Henrique, presentation on DVD):
- Live demo of compromise
- Examples: Internet website, PBX, VPN, Firewall (misconfiguration), IP Camera Systems, Oracle

PIG: Finding Truffles Without Leaving A Trace (Linn, presentation on DVD):

- @sussurro
- Wireshark data is cool but is very complicated (need to better parse the data)
- What is on a local segment? Listen vs. port scan
- Can you get user profile information easily?
- What is the network architecture?
- Focus on the broadcast and multicast (listen silently)
- This tool will be good for SysAdmin (know what is there) and IA (full picture of the network)
- Use the **Metasploit** Database fo process and manage the data
- Use **Dradis** to organize and manage results (plugin to pull from the Metasploit Database)
- Four demos – msfconsole (interface to Metasploit), db_create, db_connect, using the Wall Of Sheep Data, use PIG and set a PCAP file for review (from WIRESHARK) – RHOST – 127.0.0.1 – but run the plugin and then you data in the DB for query and review of the notes
- dradis is run via thor (connect as a client via web browser)
- Metasploit can create an XMLRPC link to their database and then thor can do the import into the DRADIS branch concept (good for navigating)
- PWN Plug Demo: small device that is full computer that looks like a power brick (control them via Ethernet, USB WIFI, cell phone) – this works with PIG – software on the device is the BACKTRACK distro
- Demo on how to build a METASPLOIT simple protocol parser for PIG
- Look at current issues: SMB; Dropbox; Groove; SSDP (Simple Sevice Discovery Protocol) – used by printers, cameras, network gateways, etc;

PacketFence: The Last Two Years (Bilodeau, presentation on DVD):

- Overview of what network access control (NAC) is and why open source is ideal of this type of product
- Uses: Perl, PHP, no agent, SNMP traps, MAC addresses, Port-Security, VLANs,
- Puts violators in a "Captive Portal"
- Can work with VoIP and provide VLAN quarantine
- Can deploy via VMWare Virtual Appliance
- A review how to bypass them: proxy, Javascript
- Roadmap review: short-term and long-term
- References listed at the end of the presentation are good

Port Scanning Without Sending Packets (Picket, presentation on DVD):

- hellfiresecurity.com
- bad guy on your network (intrusion – characterizing, profile, determine next steps)
- nbtstat (asset or intruder) // Windows hosts are pretty good put Linux and Apple require additional tool
- Multicast (mDNS) – peer to peer name resolution (part of Apple systems plus DNS-Service Discovery (224.0.0.251 via UDP 5353)

- TOOL: mDNSHostName (reverse lookup) & mDNSLookup (Q&A via IP)
- Demo (Windows cmd line tools)
- OTHER TOOLS: mDNSdiscovery, mDNSscan (captures the DNS-SD with 22 services identified over 18 ports with no scanning)
- Good video on an active scan, and then analysis
- Presenter is starting a reference library of what is found and how DNS-SD fingerprints look like (Avahi on Linux, Apple will give you the hardware model, HP printer will give you ADMIN URL, etc) ==> this will be a mDNSFingerPrint tool (TBD)
- This only works with networks with multicast and mDNS (Layer2) {probably WAN restricted}
- Sensors (today's miss this): IDS (miss this work), Etherape, Netflow/Stealwatch
- Can this be stopped? Port blocking (unmanaged will still be a problem), Application Control (yes – know what you have and what they do), Device Control (yes – good CM)
- Can NAC, ACL, & VLANs work? Already in zones of trust? ACL have some options / can break other things. VLANs can work for server/client/VoIP isolation.
- Focus on IGMP → require group membership / authentication of IGMP listeners / track membership
- You can also find all mDNS responders / disable the services or harden the box (record sanitization)
- mdnstools.sourceforge.net

Internet Kiosk Terminals (Craig, presentation on DVD):

- Review of how to hack internet kiosk systems using Kiosk Attack Tool (KAT)
- Originally released at DEFCON 16, now version 4
- Demo/Slides: On how to get in and what to try
- You can now run part of KAT payloads using Metasploit
- Demo

Overview of Attack Strategies (Crenshaw, presentation on DVD):

- irongeek.com & ISDPodcast (Thurs)
- anonymizing networks (encryption + proxies) – communication obfuscating – TOR, I2P, other networks (slides have a full list) “ciphernetworks”
- BITTORRENT doesn’t work very well on these networks
- You can end up with ISP X vs. ISP Y, or country X vs. country Y
- Good overview of TOR (proxy to interment), I2P (www.i2p2.de – hide that you are hosting within I2P, not so good for proxy to Internet)
- TOR threat – exit point sniffing (SSLStrip, plain text protocols) / man in the middle attack
- Other types of leaks: DNS (mitigate via DNS Dump on Port 53), Webbugs, HTTPS, plugins, application analysis, JavaScript
- Firefox has a socks_remote_dns setting to make sure your DNS does not link
- IRC has issues, so do all these “social” apps that log you in and then want to try to track or provide back our location information
- There are clock issues (asking for NTP) / timing issues that could be used for analysis for how many tunnels are being used (then you can compare them and find consistent time correlations)
- Metadata going into and out of the ciphernets can also be something that makes you un-anonymous

- Sybil attacks / sockpuppet – many connections (look not linked together) controlled by one person
- Traffic Analysis Attacks: timing, tagging traffic, amount of traffic, latency manipulation

Getting SSLizzard (Percoco, presentation on DVD):

- Good overview on the state of SSL (why it is used, how it is exploited)
- Man In The Middle attack tools for SSL (listed on slides)
- Mobile applications have significant issues / Mobile OS have the same problems (trust certificate issues, implementations, etc)
- TOOL: SSLizzard can be used to create "bad" certificate that can be used currently by some of the Man In The Middle attack tools (aka ettercap)
- DEMO

Network Monitoring with Arduino (Ocepek, presentation on DVD):

- in the past you had a lot of nice blinky lights – modem
- Now you don't know what is really happening
- Real time network data in LCD
- Give you a feel of what the network is doing
- Use human's natural pattern matching to detect variances project is called "cerealbox"
- Based on Atmel ATMega 328 / USB powered / serial communication (9600 – 37 msgs a second) / $30, good manual and easy to use ID // 32K of flash / 2k SRAM
- Add-on for Arduino are called "shields" … iTead Studio ($15) plus 8x8 multicolor LED Matrix ($20) so the total parts is $66
- Source code is on the DVD (perl)
- Simple Language/Protocol: command (open/close), MAC address, IP address, Ports, Country Code
- Display IP/Port connections (Green = USA, BLUE = others) – Session Mode & Meter Mode View plus new Inferno mode: port scan – nmap against you
- NET::CAP / still having an issue with Windows
- Good set of links at the end of the presentation

Network Application Firewalls (Woodberg, presentation on DVD):

- Good overview of the problem set
- Application ID is the new focus area (applications with applications)
- Working within HTTP/HTTPS
- Packet mapping and analysis is even harder with Apps within Apps
- Not having both sides of conversation also have as a more significant impact
- Obfuscation: Encryption, Tunneling, Stenography also are missed by NAC
- NAC seems to be working of keeping good applications staying good
- Malicious and "trying to hide" applications will not be stopped by NAC especially at Layer 7

Pervasive Cloaking (Manning, no presentation):

- Crypto until 1998 was considered "munitions" between most countries
- Things have changed, anonymity and privacy are important but 3rd party escrow is needed (because of law enforcement needs, etc.)

- Who is going to hold the keys and how is this going to affect multi-country situations

Tracking The Trackers (Kennish, presentation on DVD):

- Modern browsers are linking information that users are probably not completely comfortable with
- Social "widgets" are helping and reporting much of this information without disclosure
- You can track the trackers and see who is getting the most of your own information (disconnect.db)

How to build a university security team (Arpai, presentation on DVD):

- Good review of a proposed strategy on building a "cyber" workforce and to help change an organizations culture to be more security focused.

Metasploit Meets Kinect (Bryner, presentation on DVD):

- Focus: Take a Microsoft Kinect, Metasploit tools, and a 3D Game Engine and see what you can get
- Demo

Deceptive Hacking (Barnett, presentation & whitepaper on DVD)

- Pretty interesting talk on how "magicians" are a lot like "hackers"
- And how "hackers" to learn the ***tricks*** of "magicians" to be better "hackers"
- Presenter listens to PaulDotCom.com
- Demo: Walks through a scenario where a hacker targets a company using magician techniques

PXE – The "nightmare" between shutdown and boot (Weeks, presentation on DVD)

- Detailed look at how PXE (the network boot up capability) could be exploited
- This is at the BIOS level (boot firmware from the NIC)
- Uses: DHCP, TFTP
- Demo
- Also discusses how to do Offline Linux Code Injection
- List of bootkits: sinowal, stoned, whistler, TDL/alureon
- Other topics: binary embedding, DLL preloading, registry edits, pivoting,
- More demo

Email to ganesh.devarajan@gmail.com & don.lebert@gmail.com about VOIP Brief

Wireless Aerial Surveillance Platform (Tassey, presentation on DVD):

- Review of specifications: airframe, avionics, payload, base station, backend
- Review of capabilities: system topology,{movie}, base station, BackTrack 5, USRP
- Project costs (under $4K for aircraft) (under $600 for base station) (under $1K for backend)
- Review lessons' learned
- Presenters received a lot of threats
- Reality check: not as hard as it looks vs. not as easy as it looks; unforeseen problems = money; you will crash; cheap is relative
- Good list of links from the presentation for more information

Building the DEFCON network (Bryan, no slides):

- Panel (8 people)
- Intro music "Pong" Eisenfunk (8-bit)
- Secure WIFI was the main reason the network usage has increased
- Goals: reliable, secure-ish, wifi everywhere, need to create an account for the SECURE connection, they are on TWITTER (monitoring via #defcon)
- Segmentation (VLANS): public, speaker, press, greenroom, CTF network, OPSNET, Infobooth, Contests (total 49 VLANs for cable, 59 WIFI VLANs)
- Challenges: money, hotel staff (union/non-union), infrastructure (fiber, bandwidth), wireless (compatibility, density, reliable)
- MetroArea Ethernet (100-MBs) using a 1-GigBackbone
- Timeline (10 people, 7 days to setup)
- Maps: network, access points
- Diagram of network traffic and they did peak at 100-MBs twice
- Secure WIFI does not go to the wall of sheep (no peer-to-peer either)

Virtualization KVM Under attack (Elhage, presentation on DVD):

- The focus is how to break out of the Linux KVM kernel module (virtual CPU / MMU)
- Uses both Intel and AMD's virtualization extensions
- Review of known and reported bugs (some with fixes): RedHat, CVE, PCI-ISA
- Review of a timer hack
- Demo

SCADA in Prisons (Strauch, presentation on DVD):

- Review why research this topic and why it matters (plus who they have talked to already)
- Review issue at a prison where a contractor had installed the SCADA system wrong
- Small discussion on STUXNET
- Review of prison design and all have a control system (locks, doors, intercom, alarms, surveillance, etc.)
- All of this works on Programmable Logic Controller (PLCs) that are core to a SCADA system
- There are 50+ manufactures and about 9 major integration providers
- Excellent review on how SCADA system work and are designed
- Review: vulnerabilities, infection vectors, scenarios, Internet issues
- How to build a PLC Research Lab? In the slides.
- Demo

Introduction to Tamper Evident Devices (datagram, lockwiki.com, lockpickingforensics.com)

- soon tamperwiki.com
- terms: tamper resistant, proof, evident [anti-tamper sometime used]
- Seals vs. Locks: prevention vs. detection; inspection, key system costs, environmental
- Very good history in the slides (need to see if a copy is available)
- Ready "Spycraft" and "Family Jewels" for more history {BOOKS}
- Computers: Silver tamper seal on XBOX [stickers are not that effective]

- Duty Free Bags [have some different rules between countries]
- Evidence bags are another modern example
- Epoxy applied to electronics [DOD, industry, etc]
- Other examples: treaty monitoring, transportation, etc.
- Capturing tamper deployed with cameras is one of the ways to increase auditing
- Slide on inspection techniques (traps and alarms)
- Goal: open and re-seal with the least number of clues of tamper
- Review Mechanical Seals (Zip Ties, Beaded Cable Seal (Serial # vs no serial #, defeated by shim), Plunger Seal / Truck Seal (# vs. non-number, shims don't work, but removing the caps lets you get at the plunger lock area),
- Review: Padlock Seal #1 (shim, lock pick); Seal#2 (more clip like, but plastic area holds the main area, so cut it off, rust of the metal pieces off
- Review: Metal Cable Seal (see slides for diagrams) – shim can work, magnetic can also undo the lock)
- Review: Metal Ball Seal (see slides for diagrams) – complicated lock; defeat options: picking, shear, repair strap, counterfeiting [solution make new metal balls]
- Review: Bolt Seal (clip and ring configurations) – slides cover some options [DEFCON #19 Tampering solution is in video]
- Review: Roll Crimps (very easy to counterfeit) // Squeeze Crimps // Self-crimping Seals
- Cost: Detecting tampering has a cost vs. time analysis
- Plastic Wraps: defeats – shimming, cut & repair, counterfeit [depends on what the goal is]
- Adhesives: not very effective – application is misunderstood [Defeat – shimming, lifting, water, stream, solvents, temp (hot/cold), counterfeiting]
- Tape: serialized, what is attached to, backing, adhesive, residue, how much to remove
- Biggest attack; common solvents: acetone, isopropyl alcohol, carbon tetrachloride, MEK, you can look at the slides for more information
- Inspecting Adhesives – good to review the slides
- You can ruin adhesives if you use the wrong one or too much of something like heat.
- Biggest change with solvents is the “gloss” and also when you pull it off something that has been changed it will pull different