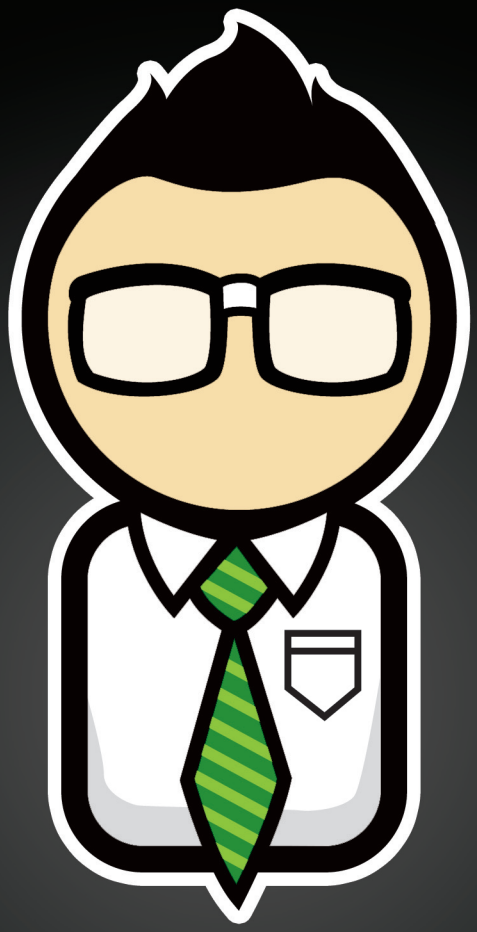
MESHCO STREAMING MEDIA Presents Point of Origin Hacking



DAYCON08

WHERE THE COOL KIDS LEARN TO PLAY

DAYCON08

WHERE THE COOL KIDS LEARN TO PLAY

SCHEDULE

Class	Day	Date	Price
ADVANCED NETWORK SECURITY	Mon-Wed	(Oct 6-8)	$3750
RFID	Wed-Thurs	(Oct 8-9)	$2750
APPSEC I	Tuesday	(Oct 7)	$1250
REVERSE ENGINEERING	Wednesday	(Oct 8)	$1250
APPSEC II	Thursday	(Oct 9)	$1250
MODERN OFFENSIVE TECHNIQUES	Thursday	(Oct 9)	$1250
VIRTUALIZATION	Wed/Thu	(Oct 8/9)	$2500

Mix and match to create your own custom training experience.
Private and after hours training available. Please inquire directly.

If you want to register or have more questions contact your sales rep or simply send an email to **pooh@meshco.com** with the subject line of TRAINING 2008. Please include the name and email address you want to register your complimentary Day-Con II ticket under. Payment details will be sent back to you via the registered email address. Methods of payment include paypal (Visa/MC/Amex/Discover), company check, certified check or money order. **Check out our website at www.day-con.org!**

DAY-CON II PASS INCLUDED FOR EACH ATTENDEE!

ASK YOUR SALES REPRESENTATIVE!

INSTRUCTORS BIOS

ENNO REY – Loves playing around with network protocols and devices since the early 90s. Prior to founding a specialized team of security researchers (aka building his own company) in 2001 he worked as a sysadmin and network operator. He has vast experience in designing, operating, troubleshooting and securing large networks and regularly contributes to the security community as a writer of whitepapers and articles, conference speaker or just as a pentester and protocol scientist.

DANIEL MENDE – Daniel is a German security researcher specialized on network protocols and technologies. He's well known for his Layer2 extensions of the SPIKE and Sulley fuzzing frameworks and has presented on protocol security at many occasions including ShmooCon, IT Underground/Warsaw and CCC Easterhegg. Usually he releases a new tool when giving a talk.

ROGER KLOSE – Roger is an experienced security geek and pentester working for Germany based ERNW. Being responsible for the overall internal infrastructure security and some parts of the security lab he's keeping his hands dirty with all sorts of gear. His main interests are in the field of intrusion detection and modern offensive techniques. He's just married and subsequently forced to develop an evolved understanding of tactical defensive approaches.

MICHAEL THUMANN - Is Chief Security Officer and head of the ERNW "Research" and "Pen-Test" teams. He has published security advisories regarding topics like 'Cracking IKE Preshared Keys' and Buffer Overflows in Web Servers/VPN Software/VoIP Software. Michael enjoys sharing his self-written security tools (e.g. 'tomas—a Cisco Password Cracker', ikeprobe—IKE PSK Vulnerability Scanner' or 'dnsdigger—a DNS information gathering tool') and his experience with the community. Besides numerous articles and papers he wrote the first (and only) german Pen-Test Book that has become a recommended reading at german universities. In addition to his daily pentesting tasks he is a regular conference-speaker and has also contributed exploit code to the Metasploit Framework. With more than 10 years of experience in computer security Michaels' main interest is to uncover vulnerabilities and security design flaws from the network to the application level.

DAYCON08

WHERE THE COOL KIDS LEARN TO PLAY

Advanced Network Sec (ANS)

INSTRUCTORS: Enno, Roger, Daniel

AUDIENCE: network designers, network operators, information security officers, internal audit

LEVEL: Medium

REQUIREMENTS: common knowledge of networking basics

TOPICS:

- Well known Security-problems on the topology-level (Sniffing, ARP Interception, Man-in-the-Middle Attacks)
- Security in Enterprise Networking
- VLANs and Security-aspects, VLAN-Hopping, VLANs with authentication
- Control Plane Protocols: Spanning Tree, CDP, HSRP, VTP, DTP
- 802.1x: When and How To Use It, examples from the real world
- Security of routing protocols: RIP, OSPF, EIGRP
- WAN/Remote Access: GRE, IPsec, Attacks against VPNs, secure configuration of BGP
- Security of network-devices: services, functions, modules, access control (RADIUS, TACACS+, Kerberos), port security
- Secure Management: security problems of SNMP, alternatives (SNMPv3, SNMP via IPsec), Logging & Log-Analyse, NTP
- MPLS: basics & security functions, VPNs with MPLS, risk analysis of MPLS VPNs
- Layer 2 Services/Carrier ethernet: Threats & Vulnerabilities, design options
- Voice over IP: security aspects and attacks, isolating VoIP

RFID Sec

INSTRUCTORS: Enno

AUDIENCE: information security officers, project managers, anyone implementing RFID based solutions

LEVEL: Medium

REQUIREMENTS: security basics, basic RFID knowledge

TOPICS:

- RFID Now! Standard RFID Now content
  - The state-of-the-art in readers, antennas and tags
  - Technology components of an RFID solution including hand-held devices, desktop printers, in-line applicators and more.
  - Current global standards and regulations
  - EPC protocols
  - RFID deployment options
  - Systems and network topologies
  - Tag type capabilities and benefits
  - Antenna types
  - Compliance requirements
  - Tag and product interactions
- Securing Production RFID Systems
- Complex System Attack Methodology (target selection/attach surface mapping)
- Network Attack Vectors
- Middleware/Application Attack Vector – Fuzzing RFID tags
- Mitigation, Remediation and Compensating Controls

DAYCON08

WHERE THE COOL KIDS LEARN TO PLAY

Application Security I (Appsec I)

INSTRUCTORS: Michael, Daniel

AUDIENCE: network designers, network operators, information security officers

LEVEL: Medium

REQUIREMENTS: knowledge of common application architectures

This course is addressed to (mainly web) applications developers and project managers with development experience. You will learn the current attack techniques of web applications, and also the required tools to detect vulnerabilities in your own systems. The countermeasures for developers are explained as well as the needful processes in application life cycle.

TOPICS:

- Common (web) application vulnerabilities and how to exploit them
- Tools & Techniques
- Practical demonstration of known vulnerabilities
- Identifying vulnerabilities (Pentesting Webapps)
- How to design complex web applications
- Planning for security mechanisms
- Secure authentication
- Security Application Life cycle
- Applications security as a business process
- Input & output validation/testing
- Basics of regular expressions
- How to secure and break applications, with practical examples from the real world

Application Security II (AppSec II)

INSTRUCTORS: Enno, Roger, Daniel

AUDIENCE: network designers, network operators, information security officers

LEVEL: Medium

REQUIREMENTS: knowledge of common application level attacks (e.g. Appsec I)

This course is addressed to (mainly web) applications developers and project managers with development experience. You will learn more advanced techniques to detect more complex vulnerabilities in your applications. The countermeasures for developers are explained as well as the needful processes in application life cycle.

TOPICS:

- Identifying vulnerabilities - the manual approach
- How to design complex web applications
- Planning for security mechanisms
- Secure authentication
- Security Application Life cycle
- Applications security as a business process
- Input & output validation/testing
- Basics of regular expressions
- Code Audit - Tools & Techniques
- Discussion of example code
- How to secure applications, practical examples from the real world
- How to break applications, with practical examples from the real world

DAYCON08

WHERE THE COOL KIDS LEARN TO PLAY

Reverse Engineering

INSTRUCTOR: Michael

AUDIENCE: pentesters, information security officers, application security people

LEVEL: High/Advanced

REQUIREMENTS: some programming knowledge

This training is for IT Security Professionals with a basic developer background. It introduces the concepts and methodologies used at ERNW for reverse engineering of closed source software under windows and also a brief introduction into the needed tools.

TOPICS:

- Needed Know How for Reverse Engineering
- Introduction of the used Toolset
- Structure of binaries (PE Header) under Windows
- The basics of disassembling
- Common problems in the disassembly process
- The basics of decompilation
- Rating and reliability of the results
- Introduction to Debugging and API Monitoring
- Advantages of API Monitoring
- Adjust the debugger to the RE project
- Runtime Analysis vs. Static Analysis
- The basics of Code Coverage
- Structured approach to Reverse Engineering
- Advantages and disadvantages of the structured approach
- Where does the approach work and where not
- Discussion of possible solutions
- Useful Addons
- SDKs for Disassembler and Decompiler
- Recommended readings and Web Links

Modern Offensive Techniques

INSTRUCTORS: Michael, Daniel

AUDIENCE: pentesters, information security officers

LEVEL: High/Advanced

REQUIREMENTS: some programming knowledge, knowledge of common attack techniques, networking skills

This workshop covers state of the art techniques to attack computer systems and networks. It will focus on client-side attacks via multimedia files, PDFs and Office documents, targeted malware spyware with advanced phone home functionality and advanced fuzzing from the OSI Layer 2 up to Layer 7. The main goal of the workshop is to provide detailed knowledge about attacks that are recently used in the wild and represent a realistic threat.

TOPICS:

- What kind of attacks are really used in the wild
- Attacking the client with all the funny stuff every user wants to see
- Circumventing counter measures like antivirus, content filter, proxies and firewalls
- Targeted Attacks
- E.T. phones home malware/spyware functionality
- How to trick the victim to run the malware
- Recent Fuzzing technologies (Layer 2 to Layer 7)
- Fuzzing Frameworks and how to extend their functionality
- Interessting Fuzzing targets

DAYCON08

WHERE THE COOL KIDS LEARN TO PLAY

Virtualization Security

INSTRUCTORS: Enno, Roger

AUDIENCE: infrastructure operators, sysadmins, information security officers

LEVEL: Medium

REQUIREMENTS: basic understanding of virtualization technologies

TOPICS:

Day 1 (Lecture)

- Major components and solutions
- Overview of attacks (Guest -> Guest, Guest -> Host, Attacks against management interfaces)
- VMBackdoor / VMEscape
- Attack Tools, Fuzzing
- The Problem "Rogue VMs"
- How to perform a risk analysis in a virtualized environment
- Basic building blocks of a virtulization security policy
- Important processes (Patching, Change Management etc.) and responsibilities

Day 2 (Workshop) VMware ESX

- Hardening and Check Lists
  - Discussion of practical attacks
- The vSwitch: security aspects, design options (Virtualized DMZs etc.), hardening
- Commercial Tools: Overview and some demos. Covers: Blue Lane, Montego, Altor
  - The role of storage virtualization & security (Blue Lane, Montego, RSA Reflex)
- Technology outlook (Flash-based Hypervisor, vSafe-Initiative)

REGISTER NOW!

If you want to register or have more questions contact your sales rep or simply send an email to **pooh@meshco.com** with the subject line of TRAINING 2008. Please include the name and email address you want to register your complimentary Day-Con II ticket under. Payment details will be sent back to you via the registered email address. Methods of payment include paypal, company check, certified check or money order.

Also check out our website at www.day-con.org!

MESHCO STREAMING MEDIA Presents Point of Origin Hacking

DAYCON08

WHERE THE COOL KIDS LEARN TO PLAY

LOCATION

Crowne Plaza Hotel Dayton, Ohio
33 East Fifth Street
Dayton, OH 45402 UNITED STATES
Hotel Front Desk: 1-937-224-0800 | Hotel Fax: 1-937-224-1231

Please be sure to register early if you intend to stay at the conference hotel. We have secured special pricing for Day-Con attendees.

Standard Room: $99.00/night
Club Level: $115.00/night
On Bedroom Suite: $250.00/night

However, you must reference the conference code: [CD8] to take advantage of the savings. If you plan on coming in earlier or staying later please let us know and we will try get the hotel to extend the discounted rates.

RFID TRAINING LOCATION

RFID Solutions Center
3001 West Tech Blvd.
Miamisburg, OH 45342
Main Phone: (937) 619-4400
Website: www.rfidsolutionscenter.com

ERNW RFID Solutions Center℠ Dayton