

Network Security Auditing:

Step into a hacker's mindset

Course Schedule – Topics & Activities

Day One

- Business risks
 - Why should you secure your external systems?
 - Privacy matters
 - Securing customer data
- Networking basics
 - Defining types of networks
 - OSI model
 - TCP/IP
- Attack & penetration overview
 - Open source testing methodology
 - How to use methodology to strategically align audits

Day Two

- "Footprinting"
 - Finding a company's Internet presence
 - Freely available information
 - Web site TMI (Too Much Information)
- Discovery
 - Identifying systems exposed to the Internet (Ping Sweeps)
 - What are those systems offering? (Port Scanning)
 - What Operating System is in use? (O/S Detection)
 - Using discovery methodologies as audit tools

Day Three

- Enumeration
 - What do the systems tell us? (auditing your public face)
 - Auditing via hacking techniques
 - Windows
 - UNIX
 - Linux
 - Web application hacking (auditing for potential holes in your eCommerce site)
- Firewalls
 - Premier & DMZ design concepts
 - Firewall options
 - Auditing firewalls

Day Four

- Auditing for common vulnerabilities & risks
 - Patches, hotfixes, & updates
 - SPAM
 - What you should be doing?

- Vulnerability management concepts
 - Independent security assessments
 - Vulnerability management applications
 - Vulnerability management appliances

*Topics and activities may vary by class and instructor.