

Marriott Courtyard (Thornton Room) -- Edmonton, Alberta

Recent newspaper stories concerning identity theft and vital records exposure are causing concerns in boardrooms across the country. How could these things happen at SOX compliant companies? The answer is that the SOX effort focused primarily on applications and transactions. Testing at the operating system and database level focused primarily on general controls. This workshop is intended for auditors who now want to make the extra effort to ensure that the systems and databases hosting SOX complaint applications are secure. With the introduction of the Canaudit audit approach, this course will show participants how to analyze security using a combination of scripts, tools, and even exploits, to identify weaknesses before they can be exploited by hackers.

Course Outline

<p>I. Understanding the Environment</p> <ul style="list-style-type: none"> • Identifying the information risks in your network • The General controls review • Physical security • Social engineering • The network scan • The initial testing and risk assessment • Determining the IT Risk Universe • Scoping the audits <p>II. The Perimeter Audit</p> <ul style="list-style-type: none"> • Identifying external connections to the network <ul style="list-style-type: none"> ✓ Dial in and out ✓ Wireless ✓ Internet ✓ Inside-out, outside-in issues • Firewalls, IPS and IDS • VPNs, Model pools, etc <p>III. The Network Audit</p> <ul style="list-style-type: none"> • Securing and segmenting the network • Network device and appliance security • Monitoring network activity • Monitoring connectivity and pattern changes • Incident response procedures and techniques <p>IV. The Windows Audit</p> <ul style="list-style-type: none"> • Identifying poorly secured machines • Determining patch levels • Passwords, the Achilles heal of Windows • Vulnerability testing • Security implementation, local and server • Audit implementation, local and server • Two factor authentication 	<ul style="list-style-type: none"> • Administration and maintenance <p>V. The Unix Audit</p> <ul style="list-style-type: none"> • Using services to take control of a system • Known exploits • Trust relationships • File insecurity • Patch and change management <p>VI. The Mainframe Audit</p> <ul style="list-style-type: none"> • So you have RACF • Securing critical libraries and files • Critical attack areas and prevention techniques • Proactive security versus reactive security • Cross environment exposures <p>VII. The Database Audit</p> <ul style="list-style-type: none"> • Excessive rights • Backdoor accounts and default passwords • Poorly secured exports and backups • Role proliferation • Remote access • Operation and maintenance <p>VIII. The Penetration Audit</p> <ul style="list-style-type: none"> • The ultimate test of preparedness • Internet and E-business exposures • Rogue Wireless access points • Undocumented dial in access • Trading partner connections • The internal test • Vulnerability assessment and conclusion <p>IX. Closing Comment</p>
--	--