Certified Virtualization Security Expert, Part 4 of 6: PenTest Tools and DMZ

Meet the expert: Duane has been working in the IT industry for over two decades. He has primarily focused on security related matters such as
Penetration Testing and Forensics. He has appeared as an expert witness in multiple court hearings on IT related matters. Duane has worked for or with most US and some foreign military branches, U.S government agencies, banking and regulatory industries and Fortune 500 companies. Duane contributed to the coordination and execution of IT counter-hacking & security courses for the US Marine Corps, US Army, US Air Force, U.S. Treasury, Sprint, IBM, Washington Mutual and Service Canada.

Tim one of the World’s leading trainers in technology, >networks, virtualization and, applications. He has been a technical trainer and consultant for security and virtualization for the past 25 years. He has 29 industry technical certifications from CISCO, Microsoft and Novell. Tim has been a noted speaker at many industry events such as Infosec World 2010, Innatech and GISSA. He is a contributing author of VMware vSphere and Virtual Infrastructure Security Securing ESX in the Virtual Environment.

Prerequisites: This is part 4 of the series.

Runtime: 02:13:46

Course description: What are the tools of a penetration test? This course will answer that as well as cover vulnerability assessment, password cracking, how to disable auditing, rootkits and alternate data streams. Then it progress to three configurations of DMZs, hardening and isolating, layer 2 security options and separation of duties. Finally threats like SSL renegotiation and web access vulnerabilities will round out the course.

Course outline:

Vulnerability Scanners
- Introduction
- BackTrack4
- Vulerability Scanners
- Nessus
- Nessus Report
- Saint
- Saint Sample Report
- OpenVAS
- OpenVAS Infrastructure and Client
- Demo: OpenVAS
- Demo: Connecting to the Server
- Demo: New Connections
- Demo: Perform a Scan
- Demo: Scan Continued
- Demo: Scan Report
- Summary

Password Cracking
- Introduction
- Windows Password Cracking
- SysKey and Cracking Techniques
- Rainbow Tables
- Disabling Auditing
- Clearing the Event Log
- NTFS Alternate Data Stream
- Stream Explorer
- Encrypted Tunnels
- Port Monitoring Software
- Rootkits
- Utilizing Tools
- Defense in Depth
- Meterpreter
- VASTO
- Summary

Pen Testing Tools
- Introduction
- VASTO Modules
- Fuzzers
- Saint
- Core Impact Overview
- Core Impact
- Tool Exploits from NVD
- Wireshark and TCP Stream Reassembling
- ARP Cache Poisoning
- ARP Cache Poisoning in Linux
- Cain and Abel
- Ettercap
- Summary

Virtualized DMZ
- Introduction
- Virtualized DMZ Networks
- Three Typical Virtualized DMZ Configurations
- Partially-Collapsed DMZ with Virtual Separation
- Fully-Collapsed DMZ
- Best Practices
- Network Labeling
- Layer 2 Security Options on Virtual Switches
- Enforce Separation of Duties
- ESX Management Capabilities
- Summary

Common Attack Vectors
- Introduction
- Common Attack Vectors
- How Fake Certificate Injection Works
- Generic TLS Renegotiation Prefix Injection
- Test Vulnerabilities
- Vulnerability Requirements
- Generic Example

(Continued on page 2)

Certified Virtualization Security Expert, Part 4 of 6: PenTest Tools and DMZ

page 2

- Patched Server with DIsabled Recognition
- Keeping Up to Speed
- SchmooCon 2010: Timeline
- SchmooCon 2010: Identification
- SchmooCon 2010: Server Log In
- SchmooCon 2010: Vulnerability
- SchmooCon 2010: Redirection Proxy
- SchmooCon 2010: Vulnerable Versions
- SchmooCon 2010: Guststealer
- Summary