Certified Virtualization Security Expert, Part 3 of 6: Penetration Testing 101

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 3 of the series.

Runtime: 03:07:01

Course description: To be secure you have to think like a hacker. This course covers penetration testing, how much hacks cost, evolving threats, information gathering, scanning, enumeration and finishes with tools that hackers and you can utilize to gather information.

Course outline:

Exploits and Malware
- Introduction
- Benefits of a Penetration Test
- The Cost of Hacks
- Cost of a Hack: Example
- Current Issues: Malware
- Zombies
- Current Issues: Zombies
- Current Issues: Botnets
- Stolen Information
- Current Issues: Social Engineering and Exploits
- Chained Exploit Example
- Gozalez Indictment
- Summary

Penetration Testing
- Introduction
- The Evolving Threat
- Methodology for Pen Testing/Ethical Hacking
- Penetration Testing Methodologies
- Different Types of Penetration Tests
- Website Review
- Demo: Security Websites
- Demo: More Security Websites
- Management Errors
- VMware Concerns
- Summary

Footprinting
- Introduction
- Methods of Obtaining Information
- Footprinting
- Footprinting Tools
- Maltego GUI
- Demo: Maltego
- Demo: Maltego Transforms
- FireCAT
- Demo: FireCAT
- Summary

Port Scanning
- Introduction
- FireFox Fully Loaded
- Google Hacking
- Advanced Query Operators
- Google Continued
- Shodan
- Demo: Shodan
- Port Scanning
- Popular Port Scanning Tools
- ICMP Disabled
- TCP Connect Port Scan and NMAP
- Half-Open Scan, Firewalled Ports, and UDP Ports
- Demo:
- Demo: Port Scanning wiht NMAP
- Demo: Perform Scan
- Demo: Discovered Ports
- Demo: Reading Output
- Summary

Enumeration
- Introduction
- UDP Port Scan
- Enumeration
- Banner Grabbing
- DNS Enumeration
- Zone Transfers
- Backtrack DNS Enumeration
- Active Directory Enumeration
- LDAPMiner
- Null Session
- Syntax for a Null Session
- Enumeration with Cain and Abel
- NAT Dictionary Attack Tool
- THC-Hydra
- Injecting Abel Service
- Demo: Cain and Abel
- Demo: ARP Poisoning
- Demo: Certificates
- Demo: Modify Port Function

(Continued on page 2)

Certified Virtualization Security Expert, Part 3 of 6: Penetration Testing 101

page 2

- Summary