

IT SECURITY

Assessment & Audit

27th & 28th March 2006 JW MARRIOTT Hotel, KL

Please Circulate To :

- CTO (Chief Technology Officer)
- CIO (Chief Information Officer)
- IT Manager
- IT Auditor
- IT & MIS Officer
- IT Security Officer

Introduction

This workshop offers a technical perspective and exposure to various audit and assessment tools and products to match the best in the industry, The primary objective being to equip participants with the skills necessary to independently conduct assessments and audits of systems/ networks.

Prerequisites

- Basic familiarity with Windows & Unix systems
- Primary understanding of networks

Event Highlights

- **Assessment & Audit- approaches & methods**
- **Network Assessment- footprint & asset identifications**
- **Discovery & Posture Mapping**
- **Information Gathering & Enumeration- Windows & Linux/Unix**
- **Attacks & Hacking- Web, Network Devices & SQL**



**FULLY PACK WITH DEMOS
& REAL LIFE CASE STUDIES**

Support by :



net-square

Endorse by :



About The Speaker

Shreeraj Shah is founder of Net Square and leads Net Square's consulting, training and R&D activities. Shreeraj is also the co-author of "Web Hacking: Attacks and Defense", published by Addison Wesley. He has published several advisories, tools, and white papers as researcher, and has presented at conferences including HackInTheBox, RSA, Blackhat, OSCON, Bellua, Syscan, CII, NASSCOM etc. His articles are regularly published on O'reilly, ZDNet, Infosecwriters etc. Previously, Shreeraj worked with Foundstone, Chase Manhattan Bank and IBM in the security space and was instrumental in product development, researching new methodologies and training designs. He has performed several security consulting assignments in the area of penetration testing, code reviews, web application assessments and security architecture reviews.

Shreeraj has a strong academic background with a Masters in Computer Science (MSCS), Masters in Business Administration (MBA) and Bachelors of Engineering (BE) in Instrumentation and Controls.



Umesh Nagori, currently, working as security consultant and trainer for the IT Security Practices at Net-Square Solutions Pvt. Ltd (hereafter referred to as Net-Square). Umesh provides information security consulting services and trainings to Net-Square clients, specializing in information security. He brings more than 10 years of experience in the Information Technology. Right from the software development, he has played key roles in various other areas of Information Technologies like system administration and network management, system analysis, training, project management. He has over 6 years of experience with web application development, application and system security architecture, network architecture, security consulting, security training. Umesh graduated from Gujarat University with a bachelor's degree in Commerce. He has also successfully completed BS7799 Lead Auditor Course.

***This Workshop is CPE Points Claimable!**

IT SECURITY Assessment & Audit

Course Outline & Arrangement

Schedule : Day 1 (27th March 2006)

08:00 **Registration**

09:00 **Module 1 Security Fundamentals and Principles**

- Security industry landscape and trends
- Security posture and evolution
- Corporate security objectives
- Threat framework and modeling
- Attack vectors and their impact
- Popular attack points and severities

10:30 **Morning Coffee Break**

11:00 **Module 2 Assessment and Audit - approaches & methods**

- Assessment methodologies and basics
- Goals and objectives of assessment
- Role of tools and credibility
- Areas of assessment & importance
- Audit basics and objective
- Compliance and standards

01: 00 **Lunch**

02:00 **Module 3 Network Assessment - Footprinting & Asset Identifications**

- Footprinting basics & objectives
- Methodologies and approaches
- Public domain queries
- WHOIS - Query all
- ARIS lookups
- DNS queries & Zone transfers
- Trace routing and mapping
- Network reconnaissance
- Windows footprinting
- Reporting and building targets

03:00 **Module 4 Discovery & Posture Mapping**

- TCP fundamentals
- Ping sweeps
- Scanning networks (TCP & UDP)
- OS identification and Stack fingerprinting
- Banner grabbing
- Protocol identification
- Network mapping
- Reporting and mapping targets

04:00 **Afternoon Coffee Break**

04: 15 **Module 5 Information gathering & Enumeration - Windows**

- Windows security overview
- Enumerating fundamentals
- Security issues with enumeration
- Windows enumeration - NetBios over TCP
- DNS enumeration
- SNMP querying
- LDAP enumeration

05:30 **Workshop Day 1 End**

Schedule : Day 2 (28th March 2006)

08:00 **Registration**

09:00 **Module 6 Information gathering & Enumeration - Linux/Unix**

- Linux/Unix security overview
- Linux/Unix systems enumeration basics
- NFS enumeration
- RPC querying
- *snmpwalk* and enumeration
- Users and groups enumeration
- SAMBA information-gathering
- *finger*, *rwho*, *rusers*

10:30 **Morning Coffee Break**

11:00 **Module 7 Attacks & Hacking**

- Password guessing, cracking & sniffing
- Privilege escalation
- Netcat shell introduction
- Other attack vectors

01: 00 **Lunch**

02:00 **Module 8 Vulnerability Assessment & Exploitation**

- Vulnerability basics
- Detecting vulnerabilities
- Vulnerability scanning using nessus & other tools
- Crafting exploits
- Exploit frameworks - Metasploit
- Countermeasures & Security

03:00 **Module 9 Web Hacking**

- HTTP protocol basics
- Web application components
- Web server assessment
- Web application profiling & hacking
- Defending web applications

04:00 **Afternoon Coffee Break**

04:15 **Module 10 SQL Hacking**

- SQL identification
- SQL banner grabbing
- MS-SQL cracking & hacking
- ORACLE cracking
- Security issues with ORACLE

05:30 **Workshop Day 2 End**