Wireless Security Training

Overview

Understand the various mobile banking models and the types of threats faced by mobile applications.

Who Should Attend?

- IT Admin who want to learn on how to audit wireless networks
- IT Admin who want to understand the attacks and defences techniques against wireless networks

Objectives

- Learns the wireless networks architecture, standard, radio transmission
- Learns the wireless network threats
- Learns the wireless auditing skills
- Understands the wireless protocols
- Familiarise the attacks techniques against wireless networks
- Learns the recommended wireless attack countermeasures

Programme Outline

Part I
(Auditing Wireless Networks)

Module 1 Wireless LAN Network Components and Architecture

- Background
- Network Types (Ad-Hoc and Infrastructure)
- Operating Modes (Managed, Ad Hoc, Monitor, Master)
- Wireless Frame and Traffic Communications
- Wireless Applications

Module 2 Wireless LAN Organisation and Standards

- FCC
- IEEE
- WiFi Alliance
- IETF

Module 3 Radio Frequency Essentials

- Understanding RF
- RF Behaviour
- Gain and Loss
- Reflection, Refraction, Diffraction and Scattering
- RF Math
- Intentional Radiator
- EIRP
- Antenna Gain
- Antenna Types
- Antenna Polarisation
- Antenna Beamwidth

Module 4 Transmission Technology

- Understanding
  - FHSS
  - DSSS
  - OFDM
- Allocated frequencies and operating characteristics
  - IEEE 802.11a network
  - IEEE 802.11b network
  - IEEE 802.11g network
  - IEEE 802.11n network

Module 5 Wireless LAN Threats

- Common Misconception and Mistakes
- The Difference between Wired and Wireless Network Security
- Wireless Protocol Deficiencies
- Information Disclosure
- Signal Exposure Threats
- Anonymity Attacks
- DoS Attacks
- Rogue AP Attack
- Home User Threats

Module 6 Wireless LAN Auditing Skills – Hands On

- Wireless LAN Auditing Toolkits and Auditing Report
- Auditing Skills 1 – Network Discovery and Sniffing
  - Using Windows Zero Configuration
  - Using Windows Preferred Network Lists
  - Using IntelPROSet Wireless Manager
  - Using NetStumbler
  - Using WiFi Hopper
  - Using Kismet
- Auditing Skills 2 – Network Mapping
  - Using knsgem and Google Earth
- Auditing Skills 3 – Finding Driver Vulnerabilities
  - Using WiFiDenum
- Auditing Skills 4 – Wireless Password Recovery
  - Using WEPKeyView
- Auditing Skills 5 – Wireless Traffic Analysis
  - Using Wireshark

<u>Part II</u>
(Defending Wireless Networks)

Module 1 Assessing WEP Networks

- Introduction to WEP Networks
- Understanding WEP technology
- Identifying and Auditing WEP Networks
- Attacks against WEP Networks
- WEP Defensive Measures

Module 2 Assessing WPA - PSK Networks

- Introduction to WPA Networks
- Understanding WPA technology
- Identifying and Auditing WPA Networks
- Attacks against WPA/WPA2 -PSK Networks
- WPA/WPA2 Defensive Measures

Module 3 Assessing WPA/WPA2 and PEAP Networks

- Risk and Challenges of Authentication Types
- PEAP Phase 1 and Phase 2 Connections
- WPA2 – PSK and WPA - Enterprise
- Attacks against PEAP Networks
- PEAP Defensive Measures

Module 4 Assessing VPN/Segmented Networks

- Typical Segmented Deployment
- Segmented Networks Features
- Weaknesses in Segmented Networks
- Identifying and Auditing Segmented Networks
- Segmented Networks Defensive Measures

Module 5 Wireless Client Exposures and Vulnerabilities

- Why Wireless Client Attacks?
- Hotspot Injection Attacks
- Publicly Secure Packet Forwarding
- Windows PNL Attacks
- IEEE802.11 Protocol Fuzzing
- Client Fingerprinting
- Client Devices Defensive Measures

Module 6 Wireless Denial of Service Attacks

- Wireless DoS Attack in Wireless LAN
- Classification of Wireless DoS I - Persistent and Non Persistent
- Classification of Wireless DoS II – PHY, MAC and Client Attacks
- Understanding PHY Attacks
- Understanding MAC Attacks
- Understanding Client Attacks
- Wireless DoS Defensive Measures

Summary

Trainer:

Mohamad Nizam Kassim, GAWN GPEN
Security Assurance Department
CyberSecurity Malaysia

Mr. Mohamad Nizam Kassim is a security assurance analyst of Security Assurance Department, CyberSecurity Malaysia for WiFi and Mobile Network technologies.

Prior to that, he has involved more than six years in telecommunication industry in designing and implementing core-switched and packet-switched network, analysing and predicting mobile network traffics forecasts, implementing core-switched network monitoring system and subscribers provisioning system.

He is currently dedicated his time in wireless station tracking and triangulation techniques project and mobile phone threats assessments project.

Fees

This programme is priced at **RM2000.00** per person, inclusive of 2-days trainer's fee, course materials, meals and refreshments, venue, parking and certificate of attendance

Venue

Training Room, CyberSecurity Malaysia, Level 4, Block C, Mines Waterfront Business Park, No. 3, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan

Duration

2 days (9:00am -5:30pm)

Registration

Download form: http://www.cybersecurity.my

Complete the registration form and fax to **+603 - 8946 0844**

Contact us
Tel: +603 – 8946 0999 Email : training [at] cybersecurity.my