TRAINING

EXPLOITING AND DEFENDING NETWORKS – ADVANCE LINUX EDITION

Trainer: Nish Bhalla – Security Compass
Duration: 2-days
Date: 18th July – 19th July, 2006
Time: 0900 hours – 1700 hours
Style: Classroom, hands-on
Cost: S$3,000 per student

Description: The purpose of this course is to provide advanced tech leads, testers, administrators, network administrators and all other participants detailed security techniques and knowledge as applied to Network security and Host Security. It is focused towards helping users understand how to find and write basic stack based exploits. Participants will also learn how to take advantages of vulnerabilities that might exists in an environment and use backchannels to connect back into a network. Hands-on lab exercises reinforce the course material in a real world environment.

Pre-requisite: Basic knowledge of programming on Windows or Linux is a pre-requisite. Having knowledge of using an editor like vi or Emacs and having the knowledge of compiled using Gcc / Visual Studio is a pre-requisite.

All students will be required to bring their own laptop; and must have administrative access on their laptops to install software. VM-Player (http://www.vmware.com/products/player/) will be installed. Windows/Linux images will be provided for use during the class. It is recommended that the laptops have 512 MB of RAM.

Class Outline:

Part I - Introduction to Buffer Overflows
- Buffer Overflows (Linux)
  - Basics of Stack
  - Assembly basics
  - Understand stack overflows
  - Exploiting local stack overflows
  - Writing a local stack overflow

Part II – Wireless
- Basics of Wireless Hacking
  - How to Find Wireless Networks.
  - Breaking WEP/WPA/LEAP
  - Setting up a Fake AP (Either on Linux / Linksys WRT54GL)

Part III – Network Scanning and Back Channels
- Network Scanning & Hacking
  - Advanced Port / Network Scanning techniques
  - MITM Attacks
  - SSL MITM Attacks
  - SSH MITM Attacks
  - DNS Spoofing Attacks

- Ettercap to the Rescue
- TCP Hijacking

Back Channels [Methods of hiding and bypassing firewalls]

- Bash Shell Based Back Channels
- XML Based Back channels
- HTTP Based Back channels
- MSN Based Back Channels

PRACTICAL WIFI (IN) SECURITY

Trainer: Cedric “Sid” Blancher – EADS Research
Duration: 2-days
Date: 18th July – 19th July, 2006
Time: 0900 hours – 1700 hours
Style: Classroom, hands-on
Cost: S$3,000 per student

Description:

Pre-requisite:

Class Outline:
- 802.11 Introductions
  - Physical consideration
  - Frame format
  - Basis and functionalities
- 802.11 Insecurity
  - Intrinsic flaws
    - Jamming
    - Enumeration/identification (wardriving)
    - Management traffic injection + HANDS-ON
    - RogueAPs + HANDS-ON
- WEP
  - Crypto/RC4 reminder
  - WEP data encryption and authentication
  - WEP flaws identification
  - WEP flaws exploitation and cracking + HANDS-ON
- Traffic injection based attacks
  - Open & WEP infrastructure abuse
  - Captive portal bypass + HANDS-ON
  - Clients attacks and isolation bypass + HANDS-ON
  - Ad hoc mesh networks attacks
- 802.11 Security
  - Flaws to address identification
  - Solutions
    - 802.1x and EAP
    - WPA
    - 802.11i/WPA2
  - Configuration guidelines
    - WPA/WPA2 support for AP, adapters and OS
    - Tricks : PSK vs. EAP, WPA vs. WPA2, TKIP vs. AES
    - Architecture thoughts
- HANDS-ON
  - Configuring WPA/WPA2 STA
  - Configuring WPA/WPA2 AP/Authenticator
- Conclusions
  - Kiss and goodbye :)

DEFENDING WEB APPLICATIONS

Trainer: Nish Bhalla – Security Compass
Duration: 2-days
Date: 18th July – 19th July, 2006
Time: 0900 hours – 1700 hours
Style: Classroom, hands-on
Cost: S$3,000 per student

Description: The two day course is an intense course in understanding how to defend web application attacks. The goal is to provide tech leads and developers, detailed security techniques and knowledge as it applies to web application security. The training introduces the concepts of web application security, the latest techniques in exploiting web applications, and most important of all teaches hands on defending web application. Participants will learn JSP and ASP.NET vulnerabilities, as well as learn how to securely write web applications in ASP.NET and JSP. This is a complete hands-on class where the concepts are re-enforced by labs based on real world environment.

Pre-requisite: Knowledge of programming in JSP or ASP.NET environment is required.

All students will be required to bring their own laptop; and must have administrative access on their laptops to install software. VM-Player (http://www.vmware.com/products/player/) will be installed. Windows/Linux images will be provided for use during the class. It is recommended that the laptops have 512 MB of RAM.

Class Outline: Part I -

Introduction
Introduction to Web Servers
- HTTP
- SSL Basics Explained

Introduction to Web Applications
- Server, application (client [include js] and server), infrastructure modules (DB, etc)

Understanding Web Applications Architecture
- Detailed Description of web application components.
- Methods of Authentication
  - Basic Authentication
  - Forms Based Authentication
- Cookies (components)
- Session Management
  - Using Session IDs (also non cookie approach, manual) to maintain sessions.
- Access Control
- Encryption
- Data Validation
- Logging

Principles of Secure Web Application Development
Threat Analysis

PART II - Attacking the Web Server

Foot-printing

- Banner Grabbing [Hands On]
  - Netcat (GET)
  - nmap
- Automated Web server scanning
  - nikto / stealth [Hands On], nikto over SSL [Hands On]
  - wikto
- Mis-configurations
  - Directory Listings
  - Web server statsitics (/stats)
  - Default installations and sample scripts
- Unmapped File Handlers
  - Include files (.inc, .conf*, *.bak, *.tar.*, *.zip, etc)
  - Source code disclosure (.asp, .php, .cgi, .java, etc)

Misc. Server Attacks

- Buffer Overflows (IIS and Apache vulns)
- Introduce Metasploit [Hands On]
- Decompiling .class (JAD) [Hands On] and .NET assemblies
- Decompiling proprietary DLLs

Hardening the environment

PART III - Defending Application

Most of the time is spent in finding the vulnerability in reviewing code and rewriting the code to fix the vulnerability. The focus is to learn where the major mistakes are commonly made and how to fix them in a typical ASP.NET and J2EE web application.

Authentication

- User enumeration
- Brute Forcing
  - Exploiting "Forgot Password?" features
- Session Management
  - Cookie and Session Manipulation (Incrementing Session IDs)
- Encode vs. Encrypt

Implementing Authentication across a domain are discussed and vulnerable source code is reviewed to find defects in authentication implementation (LDAP/Forms Based).

Authorization & Session Management

Review Code and find defects in session management implementations

Data Validation

Issues such as cross site scripting, field overflows, SQL Injection are covered as well as how to defend against those vulnerabilities are coded.

Error Handling (eXploiting & Defense)
Techniques of taking advantage of Error Messages, defending against error messages

Exploiting Application Logic

- How it works (Example: Negative integers and inputs).
- Difficult to Detect
- HTML Hidden Fields
- Client side length and server side length of variables
- File upload (example: Bad extensions, browser attacks)

Take Home:

Secure Coding Practices guide to JSP and ASP.NET will be provided.

ADVANCED HONEYPOT TACTICS

Trainer: Thorsten Holz – Aachen University
Duration: 2-days
Date: 18th July – 19th July, 2006
Time: 0900 hours – 1700 hours
Style: Classroom, hands-on
Cost: S$3,000 per student

Description: Honeypots or their younger brother Honeynets are very much en vogue nowadays. Firewalls, VPNs, IDS, IPS - are honeypots the next big hype? This two day course explains what honeypots are, what they are good for, when they can bring rapid ROI to an organization deploying them and when they are only of academic interest.

This course will teach how to setup different types of honeypots and how to learn more about the tools, tactics, and motives of blackhats. In addition, the course also shows how to swiftly detect and react to malware outbreaks in an organization. Moreover, it will be demonstrated how honeypot technology can be used to estimate risks in a way management understands. This course shows how to use honeypot technologies as a concrete improvement to your organisations security defences, combined with many hands-on exercises.

Pre-requisite: Students should have a basic understanding of the concept behind honeypots. Moreover, having knowledge of programming on Linux and a good understanding of TCP/IP networking is helpful. All other material will be briefly introduced during the class.

Class Outline: Part I - Honeypots

- Introduction to high- and low-interaction honeypots /honeynets
- Gen III honeynets
- Web-based honeypots
- Hands-on exercises
  - Case study: Learning more about phishing

Part II - Honeyd

- Working of honeyd
- Routing traffic to honeyd
- Simulation of TCP/IP stacks / network infrastructure / applications
- Advanced honeyd configuration
- Centralized data collection with honeyd
- Writing honeyd plugins
- Protecting corporate network infrastructure with honeyd

Part III - Collecting malware with honeypots

- Techniques used
- mwcollect / nepenthes
  - How they work
  - Writing your own modules
  - Analyzing the received shellcodes
  - Analyzing the captured binaries
- Results

Part IV - Bots/Botnets

- Introduction to bots and demo
- Reverse engineering of bot
  - Basic techniques
  - Sandboxes
  - Ollydbg and/or IDA
- Botnet 101
  - How they work
  - What you need to know
  - Observing them
- Live botnet observation
- Results