Hands-On

Beating Hackers Today: Intrusion Analysis, Detection & Protection

Course Description

Considerable concern has resulted from reports that Google, and what has been reported as more than 20 other companies, have fallen under hacking attacks thought to emanate from China. There is nothing special about news of hacking. What has changed is the recent realization that it is likely that the latest breed of hacker is no longer an individual amateur wanting to prove their individual skill as a challenge, but may well be serious government funded professional group. It is thought that attacks have been perpetrated on commercial, banking and defense corporations as well as high profile Internet businesses like Google and Yahoo.

With potential in the future from terror groups as well, detecting attempted intrusions attacks early and effectively is critical, not just to protect human rights, as was thought to be the motivation for the Google attacks but also to protect major commercial Interests and national security. Detecting potential attacks and being aware of likely threats is important to all organizations. It is no longer just security experts that need security skills, but it should be within the knowledge base of all technical professionals.

This course provides an understanding of the jargon that surrounds this field. It analyzes the different classes of attack that have been identified and examines some of the methods that have been employed by hackers. Having established the form of the threats it teaches how to detect and recognize these threats without crippling the networks being defended. It then goes on to establishing countermeasures and good practice to minimize or remove the threats.

Students learn the inner workings of the "real" TCP/IP protocols from intrusion detection points of view. In addition to studying the normal or expected TCP/IP conventions and behavior the course examines malicious or unexpected patterns that may be seen in the wild. This provides participants a more accurate view of real world situations that they would encounter and prepares them to determine what is going on in the actual network traffic. WireShark is used to produce an audit trail of traffic flowing in and out of the network and allows packet content to be analyzed for abnormalities. Students learn how to recognize the warnings and alerts produced by intrusion detection systems and determine the source of problem as well as capturing pertinent activities afterwards. Hands-On exercises on analysis tools are used to achieve this.

The course finally goes on to examine how Intrusion Detection Systems can be deployed to automate detection and potentially undertake countermeasures to protect.

Students Will Learn

- **Footprinting**
- **Network scanning**
- **Enumeration**
- **Packet sniffing**
- **Social Engineering**
- **DoS/DDoS**

- **Session hijacking**
- **Webserver and web application attacks and countermeasures**
- **SQL injection attacks**
- **Wireless encryption**
- **Cloud computing threats**
- **Cryptography ciphers**
- **Penetration testing**
- **Describe The Mechanisms Most Often Used In Serious Hacking Attacks**
- **Identify Threats Using Protocol Analysis And Detection Tools**
- **Analyze Network Traffic To Locate Service Attacks**
- **Implement Countermeasures To Mitigate Or Prevent Attacks**
- **Plan Methods For Testing And Audit The Effectiveness Of Countermeasures**
- **And More...**

Target Audience

Anyone the is interested and responsible for protecting their network environment, whether it be personal or business.

Prerequisites

This course assumes attendees already have basic knowledge of data communications, PCs and IP systems.

Course Outline

Module I: Survey of Hacking Attacks

High profile attacks detected recently

Classification of threats

Eves Dropping

Back Doors

Virus attacks

Worms

Phishing Attacks

Port Scanning

Password Scanning

Man-in-the-middle attacks

Denial of Service

Module II: Review of Security

Review of layered protocols

Application and network service layers

Identifying Ethernet security issues

Addressing Issues

Ethernet Addressing

IPv4 addressing

Analyzing IP fragmentation

Identifying ICMP security issues

Implementing basic traffic capture and analysis

Module III: IP and ARP Vulnerability Analysis

Identify IP security issues

Describe IP routing and routing protocol security

Protect against IP abuse

Identify ARP security issues

Execute attacks against ARP

Protect against ARP abuse

Implement advanced packet capture and analysis

Module IV: UDP/TCP Protocol Vulnerability Analysis

Discuss characteristics of UDP and TCP

Identify TCP security issues

Common TCP abuses:

SYN attack, sequence guessing, connection hijacking

Discuss characteristics of TELNET

Identify TELNET security issues

Execute attacks on TCP and TELNET

Protect against TCP and TELNET abuse

Module V: FTP and HTTP Vulnerability Analysis

Characteristics of FTP

Analyzing FTP transfer methods and modes

Identifying FTP security issues

Common FTP abuses: FTP bounce attack, port stealing, brute force

Characteristics of HTTP

HTTP proxy servers and HTTP authentication

Identifying HTTP security issues

HTTP abuses: path name stealing, header spoofing, proxy poisoning

Attacking FTP and HTTP

Protecting against FTP and HTTP abuse

Module VI: DNS Vulnerability Analysis

Characteristics of DNS

Identifying DNS security issues

DNS abuses: DNS spoofing, DNS cache poisoning, unauthorized zone transfers

Attacking DNS

Protecting against DNS abuse

Module VII: SSH and HTTPS Vulnerability Analysis

Characteristics of SSH

Differences between SSH1 and SSH2 protocol

Identifying SSH security issues

SSH abuses: insertion attack, brute force attack, CRC compensation attack

Characteristics HTTPS (SSL)

Other SSL enabled protocols

Common SSL abuses: man-in-the-middle and version rollback attack

Module VIII: Network Attack Techniques and Basic Attack Detection

Identify sources of network attacks

Discuss methods of intrusion

Describe common network attacks: denial-of-service, software buffer overflow, poor system configuration, password guessing/cracking

Describe a typical intrusion scenario

Introduce the concept of an Intrusion Detection System (IDS)

Some popular IDS tools: Snort, Security Center, ThreatSentry

Implement basic scan detection

Types of IDS implementation: hybrid NIDS and honeypots

Components of a NIDS using the snort NIDS

Advanced features: "real time response" and log monitors

Module IX: Intrusion Risk Minimization and Best Practice

Top 7 key actions to take

Elements in staff best practice

Controlling Keys, passwords and permissions

Separation of Services

Actions for Audit

Evaluation and Review

Delivery Method

Instructor-Led with numerous case-studies and Hands-On exercises.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

3 Days