Running head: ETHICAL HACKING: Teaching Students to Hack

Ethical Hacking: Teaching Students to Hack

Regina D. Hartley

East Carolina University

Abstract

One of the fastest growing areas in network security, and certainly an area that generates much discussion, is that of ethical hacking. The purpose of this study is to examine the literature regarding how private sectors and educational institutions are addressing the growing demand for ethical hacking instruction. The study will also examine the opportunity for community colleges in providing this type of instruction. The discussion will conclude with a proposed model of ethical hacking instruction that will be used to teach a course in the summer semester of 2006 through the continuing education department at Caldwell Community College and Technical Institute within the North Carolina Community College System.

Ethical Hacking: Teaching Students to Hack

The growing dependence and importance regarding information technology present within our society is increasingly demanding that professionals find more effective solutions relating to security concerns. Individuals with unethical behaviors are finding a variety of ways of conducting activities that cause businesses and consumers much grief and vast amounts annually in damages.

As information security continues to be foremost on the minds of information technology professionals, improvements in this area are critically important. One area that is very promising is penetration testing or Ethical Hacking.

The purpose of this paper is to examine effective offerings within public and private sectors to prepare security professionals. These individuals must be equipped with necessary tools, knowledge, and expertise in this fast growing proactive approach to information security. Following this examination a proposed model of Ethical Hacking instructional plan will be addressed.

Ethical Hacking

One of the more effective ways of testing network security is penetration testing or ethical hacking. Activities focus on the identification and exploitation of security vulnerabilities, and subsequent implementation of corrective measures (Using an Ethical Hacking Technique). Organizations are increasingly evaluating the success or failure of their current security measures through then use of ethical hacking processes. According to some "'ethical hacking' may be one of the most effective ways to proactively plug rampant security holes" (Yurcik & Doss, 2001). Moreover, many security experts encourage organizations to hire ethical hackers to test their networks (Leung, 2005).

According to those within the security field, more information technology professionals going back to class to learn the "latest hacking techniques." In fact, many consider the three to five day seminars to be less expensive than hiring consultants. The average cost is $2,000 to $8,000 per person while consulting services range from $10,000 to $100,000 (Slania, 2003).

According to the 2005 Computer Crime and Security Survey, virus attacks continue as the source of greatest financial loss. Unauthorized use increased slightly over the previous year, while unauthorized access to information and theft of proprietary information significantly increased in average dollar loss per respondent. Even more alarming, web site incidents have increased significantly over the previous year (CSI/FBI).

Ethical Hackers

Many individuals have a far different perception of hackers. Hackers, in reality are much different from the individuals responsible for the computer attacks and viruses of today. A hacker may be defined as a ”person who enjoys learning the details of computer systems and how to stretch their capabilities….One who programs enthusiastically or who enjoys programming rather than just theorizing about programming” (Ethical Hacking: Student courseware)**.** Ethical hacking may be defined as the “methodology adopted by ethical hackers to discover the vulnerabilities existing in information systems’ operating environments” (Using an Ethical Hacking Technique).

There are a number of categories of hackers such as Black Hats who are highly skilled, but have malevolent and detrimental intent. White Hats, in contrast, are hackers who use their talent to protect and defend networks. Gray Hats hack for different reasons

either ethically or unethically depending on the situation and circumstances at hand (Ethical Hacking: Student Courseware).

Ethical Hacking Education

A wide range of educational opportunities exist for individuals interested in pursuing information security. Many of these are being offered in the public sector within community colleges and universities. It is interesting to note that while many schools offer such education and training, a number of professionals express concern about teaching hacking techniques. This apprehension stems from a fear that students may use the information unethically. Educational institutions counteract this assumption by offering concepts within an ethical framework (Sanders, 2003).

Community Colleges and Universities

Some of the more prominent programs at community colleges and universities vary in intensity and course content. Syracuse University offers a Cyber Security Boot Camp to prepare future technology security professionals. Topics include cybersecurity, cryptography, steganography, digital forensics, network security, and wireless security. There are stringent rules for entry into the program, and the Boot Camp ends with "Hackfest" which is a hands-on event putting into practice the theoretical concepts covered within the course (Carnevale, 2005).

In Paris, Zi Hackademy, offers hacking courses to a wide variety of students. The school's philosophy is "only if you become a hacker can you understand how hackers think and operate" (van der Laan, 2001).

The University of Glamorgan and a leading information security firm 7Safe offer certifications in penetration testing and information security with additional topics

addressing wireless security and computer forensics (New Standard in Ethical Hacking).

In Los Angeles, a college is offering a course to prepare students to be able to pass the Ec-Council's Certified Ethical Hacker exam. The cost per student is $4,000 (Berkowitz, 2004).

To help government and businesses minimize security risk, colleges and universities are increasingly offering courses and security training programs. At Rochester Institute of Technology, for example, courses in security education has been added to the curriculum. Students are divided into two teams; they set up networks and try to hack each other. As security flaws are found, they patch their systems and continue to secure the networks more and more as the semester progresses (Thurrott, 2005).

At another college, Northern Virginia Community College, offers a network security certificate program. Leaders at the college interviewed their community and found that people were being educated at "too high of a level," and programs were needed to help day-to-day security professional. There are 7 courses, 3 theory and concept, 3 labs, and a capstone course. The capstone is a free vulnerability analysis of a local non profit organization or small business. The capstone is important in that it provides a hands-on opportunity to put into practice everything learned in the classroom (Thurrott, 2005).

George Mason University also offers a course in information warfare. Students divide into different country teams, and attempt to hack into each other's network. The course motto is that "anyone can hack but defending a system is the real mark." At Highline Community College the focus is a little different in that coursework focuses on data recovery. All the colleges and universities suggest the same recommendation for

programs and that is hacking must be taught within an ethical framework. Ethical hackers are the final product, and students learn network security with a hacker's mindset (Thurrott, 2005).

A researcher from Weber State University reviewed 36 schools chosen as Centers of Excellence in Information Assurance Education by the United States National Security Agency to create a security program. The program is provided by the National Security Agency to help prepare individuals for careers in information assurance and computer security. The researcher concluded his study by suggesting a capstone course to provide a "hands-on" application, and suggested that only seniors be admitted into the program only after they sign a code of ethics (Logan, 2002).

Ethical Hacker Certification Boot Camps

The private sector has been very successful at offering a vast array of educational programs for security professional. Many firms offer "boot camps" lasting from 5 to 10 days and costs range from $2000 to $5000. A marketing research group, IDC, projects that the number of security professionals will grow to over 800,000 by 2008, and according to many professional "more of them need to think like hackers to be effective" (McGee, 2005).

Intense School also provides "ethical-hacker boot camps" as well as The Academy, NetCom Information Technology, and CertificationCity. The leading supplier of the certification program for ethical hacking is Ec-Council. They boast of the C|EH (Ethical Hacking Certification) as being the "fastest growing certification in the security industry." Their program contains 22 modules that cover a variety of topics, techniques, and hacking tools (Ethical Hacking: Student courseware).

The United Kingdom is offering their first hands on ethical hacking course called The Training Company. A variety of topics are included such as social engineering techniques, wireless security, internal hacking, denial of service attacks, and penetration testing. The leaders of the program protest that unethical individuals are not attracted to the course due to the high cost of the program and the availability of free hacking tools and web sites on the Internet. In addition, applicants to the program must sign a legally binding document in which they agree to use their skills for only ethical and legal activities (Goodwin, 2004).

A group of individuals called the Ghettohackers are trying to change way society views hackers. They enable people that are curious about information security to get hands on experience without any harm to others. Their mission is to change culture from within and to better educate the public at large concerning hacking. In addition, their main focus is to stress the importance of teaching ethics as well general hacking concepts (Lemos, 2002).

One young man, Ankit Fadia, has co-founded an organization called e2Labs that offers ethical hacking courses. Mr. Fadia has authored a number of books on the topic. The objective of the e2Lab is to train individuals with the skills necessary to protect the information technology assets of his country through education, technology, and experience (e2Labs to set up Asia's first school).

One organization, ISECOM, provides hacker re-training. They bring together the positive elements of hacking as well as business disciplines. Their programs cross train hackers with business managers to promote security and privacy awareness (Non-profit provides hacker re-training).

Another program offered by ISECOM is the “Hacker High School” project. This programs offers “security and privacy awareness teaching materials and back-end support for teachers of elementary, junior high, and high school students." Developers of the Hacker High School project are interested in training a "new breed of ethical hacker," and believe there are many job opportunities available. Some of the topics included in the program are Being a Hacker, Windows and Linux, Ports and Protocols, Services and Connections, System Identification, Malware, Attack Analysis, Digital Forensics, E-mail Security and Privacy, Web Security and Privacy, Passwords, and Internet Legalities and Ethics (Hackerhighschool.org).

Recently Columbia, South Carolina delivered a Certified Ethical Hacking course to provide clients with state-of-the-art security training. Their course covers over 400 hacker tools, 300 security tools, 2500 pages of course material, and 120 classroom hands-on hours (Certified Ethical Hacking).

Platform for Ethical Hacking Education

The community college offers a unique opportunity for educational leaders to provide ethical hacking instruction. There are a number of reasons why the community college system is particularly well suited to offer ethical hacking instruction. The community college serves a diverse student population more reflective of and better representing the adult population, and has an opportunity to reach greater numbers of the population. The highest growth has occurred in two-year colleges as compared to four-year universities, and lead in offering welfare reforms and increased literacy levels. In addition, the community college system is more reflective of the community it serves and has the ability to be more adaptive to the needs of the people (DeLisse, 2000).

It is predicted that community colleges will be better able to respond to the changing demands of information technology than other educational institutions. The reasons include: growing competition from the private sector, growth of nontraditional delivery integrated with traditional campus-based programs, and the changing role of the teacher from dispenser of knowledge to facilitator of learning. In addition, "just-in-time learning" and "just-in-time training" will increase and change expectations. Finally, community colleges are expected to assume a leadership role in managing the effects of societal changes due to their relationship and role within the community (North Carolina Community College System, 1999).

Proposed Course Outline and Instructional Plan

A course in Ethical Hacking is planned for the summer semester 2006. It was decided that Ec-Council's recommended program would be followed for the course content. This program consists of 22 separate modules covering a wide variety of topics such as ethics and legality, footprinting, scanning, enumeration, and system hacking to name a few. Students will receive the course content through lecture and discussion for the theoretical concepts, and they will put the concepts into practice through the use of hands on lab applications. Featured hacking tools will be utilized in addition to other penetration measures as outlined within featured texts. In addition to the Ethical Hacking Student Courseware text, three additional books will be used in the course. The final component of this course will utilize testing preparation materials to assist students in applying their knowledge to become a Certified Ethical Hacker. The course outline is provided for additional information (see Appendix).

Conclusion

Effective ethical hacking course offerings are being provided by colleges and universities as well as "boot camps" offered by private organizations. A variety of programs indicate a wide array of content, target audience, cost, and duration. The community college system provides a very effective platform for offering ethical hacking course concepts and applications. A proposed model for ethical hacking instruction was discussed and is planned for the summer semester of 2005. After completing this course students will be better prepared to become Certified Ethical Hackers and contribute to the security field.

References

10th annual computer crime and security survey. CSI/FBI 2005. Retrieved April 15, 2006 from gocsi.com.

Berkowitz, B. Hacker college. (2004, July 7). Retrieved April 5, 2006 from http://smh.com.au/

Carnevale, D. (2005, September 23). Basic training for anti-hackers: An intensive summer program drills students on cybersecurity skills. Chronicle of Higher Education, 52(5), pp. 41-41.

Certified Ethical Hacking. Retrieved April 5, 2006 from www.wistv.com

DeLisse, R. L. (2000). Rationale for computer ethics policies and a model policy for the North Carolina Community College System. (ERIC Document Reproduction Services No. ED 457932).

e2 Labs to set up Asia's first School for ethical hacking in Hyderabad. Retrieved April 5, 2006 from www.reachouthyderabad.com

Ethical Hacking: Student courseware. Ec-Council. www.eccouncil.org

Goodwin, B. (2004, March 16). Hacking course offers insights into the mind and method of bad guys. Computer Weekly. Retrieved April 5, 2006 from www.trainingcamp.co.uk

Hacker High School. Retrieved April 5, 2006 from www.hackerhighschool.org

Lemos, R. (2002, August 2). Hacking their image: Underground school tries to reprogram reputation. Retrieved April 5, 2006 from CNet News.com.

Leung, L. (2005, June 20). Hackers for hire: Bringing in ethical hacker consultants is the latest in security defense. Retrieved November 5, 2005 from http://www.networkworld.com.

Logan, P. Y. (2002). Crafting an undergraduate information security emphasis within information technology. Journal of Information Systems Education, 13(3), pp. 177-182 2002

McGee, M. K. (2005, June 23). Hacker boot camp helps good guys outsmart internet troublemakers. Retrieved November 20, 2005 from http://www.informationweek.com.

New standard in ethical hacking: University and industry partnership creates new qualification. (2005). Retrieved April 5, 2006 from http://www.m2.com

Non-profit provides hacker re-training. (2004) ISECOM. Retrieved April 5, 2006 from www.isecom.com

North Carolina Community College System fact book. (1999). Raleigh, NC: North Carolina Community College System [On-line]. Available: http://www.ncccs.cc.nc.us

Sanders, A. D. (2003). Utilizing simple hacking techniques to teach system security and hacker identification. Journal of Information Systems Education, 14(1), p. 5.

Slania, J. (2003, April 28). Courses teach lessons in hacking. Crain's Chicago Business, 26.

Thurrott, S. Anyone can hack; it's defending the system that's cool. Retrieved November 20, 2005 from http://www.course.com.

Using an Ethical Hacking Technique to Assess Information Security Risk. (2003). The Canadian Institute of Chartered Accountants. Retrieved November 20, 2005 from http://www.cica.ca/itac.

van der Laan, N. (2001, December 3). Hackademy: Paris school offers primer for cyberpirates. Christian Science Monitor, 94(7).

Yurcik, B. S., Doss, D. (2001). Ethical hacking: The security justification. Ethics of Electronic Information in the 21 Century Symposium. University of Memphis: Memphis TN.

Appendix

Certified Ethical Hacking Course
Course Outline

Course Description

This class will follow Ec-Council's recommended 22 module learning system to prepare students for the EC-Council Certified Ethical Hacker exam 312-50. Students will receive course content information through a variety of methods. Lecture and demonstration of hacking tools will be used in addition to an interactive environment. Students will receive a hands-on practical approach in penetration testing measures and ethical hacking. No text book is required for students; however, four books will be utilized for course content and students may wish to purchase any or all for personal and professional use. The final component of this course will utilize testing preparation information, and students will be able to apply their knowledge to become a Certified Ethical Hacker. The course is composed of 15 class sections as outlined below.

Textbooks Used:

1) Ethical Hacking: Student Courseware
Ec-Council
ISBN 0972936211

2) Hands-On Ethical Hacking and Network Defense
Michael Simpson
ISBN: 0-619-21708-1 © 2006

3) The Unofficial Guide to Ethical Hacking, Second Edition
Ankit Fadia
ISBN: 1-59863-062-8 © 2006

4) Network Security: A Hacker's Perspective
Ankit Fadia
ISBN 1592000452

Class Section 1

Module 1: Ethics and Legality

- Why Security?
- The Security, functionality and ease of use Triangle
- Can Hacking be Ethical?
- Essential Terminology.
- Elements of Security.
- What does a Malicious Hacker do?
- Difference between Penetration Testing and Ethical Hacking.

- Hacker Classes.
- What do Ethical Hackers do?
- Skill Profile of an Ethical Hacker.
- Modes of Ethical Hacking.
- Security Testing.
- Deliverables.
- Computer Crimes and Implications.
- Legal Perspective (US Federal Laws).

Module 2: Footprinting

- Defining Footprinting.
- Information Gathering Methodology.
- Locate the Network Range.
- Hacking Tools:
  - Whois
  - Nslookup
  - ARIN
  - Traceroute
  - NeoTrace
  - VisualRoute Trace
  - SmartWhois
  - Visual Lookout
  - VisualRoute Mail Tracker
  - eMailTrackerPro

Class Section 2

Module 3: Scanning

- Definition of Scanning.
- Types of scanning
- Objectives of Scanning
- Scanning Methodology
- Classification of Scanning
- Hacking Tools
  - Nmap
  - XMAS Scan
  - FIN Scan
  - Null Scan
  - Windows Scan
  - Idle Scan
  - Nessus
  - Retina
  - Saint
  - HPing2
  - Firewalk
  - NIKTO
  - GFI Languard
  - ISS Security Scanner
  - Netcraft
  - IPsec Scan
  - NetScan Tools pro 2003
  - Super Scan

    - Floppyscan
- War Dialer
- Hacking Tools
    - THC Scan
    - Friendly Pinger
    - Cheops
    - Security Administrator's Tool for Analyzing Network (SATAN)
    - SAFEsuite Internet Scanner
    - IdentTCPScan
    - PortScan Plus
    - Strobe
    - Blaster Scan
- OS Fingerprinting
- Active Stack fingerprinting
- Tool for Active Stack fingerprinting
    - XPROBE2
- Passive Fingerprinting
- Proxy Servers
- Hacking Tools
    - Socks Chain
    - Anonymizers
    - HTTP Tunnel
    - HTTPort
- Countermeasures

Class Section 3

Module 4: Enumeration

- What is Enumeration?
- NetBios Null Sessions
- Hacking Tools
    - DumpSec
    - Winfo
    - NetBIOS Auditing Tool (NAT)
- Null Session Countermeasures
- NetBIOS Enumeration
- Hacking Tool :NBTScan
- Simple Network Management Protocol (SNMP) Enumeration
- Hacking Tools
    - Solarwinds
    - Enum
    - SNScan
- SNMP Enumeration Countermeasures
- Management Information Base (MIB)
- Windows 2000 DNS Zone Transfer
- Blocking Win 2k DNS Zone Transfer
- Enumerating User Accounts
- Hacking Tools
    - User2sid and Sid2user
    - UserInfo
    - GetAcct
    - DumpReg
    - Trout

- Winfingerprint
- PsTools (PSFile,PSLoggedOn,PSGetSid,PSInfo,PSService,PSList,PSKill,
  - PSSuspend, PSLogList, PSExec, PSShutdown)
- Active Directory Enumeration and Countermeasures

Class Section 4

Module 5: System Hacking

- Administrator Password Guessing
- Manual Password Cracking Algorithm
- Automated Password Cracking
- Password Types
- Types of Password Attacks
- Hacking Tool
  - NTInfoScan (CIS)
- Performing Automated Password Guessing
- Hacking Tool

* Legion
  - Password Sniffing
* Hacking Tools
  - LOphtcrack
  - pwdump2 and pwdump3
  - KerbCrack
  - NBTdeputy
- NetBIOS DoS Attack
- Hacking Tools
  - NBName
  - John the Ripper
- LAN Manager Hash
- Password Cracking Countermeasures
- Syskey Utility
- Cracking NT/2000 Passwords
- Hacking Tool
  - NTFSDOS
- SMB Logon
- Hacking Tool: SMBRelay
- SMBRelay Man-in-the-Middle Scenario
- Hacking Tool : SMBRelay2
- SMBRelay Weaknesses and Countermeasures
- Hacking Tools
  - SMBGrind
  - SMBDie
- Privilege Escalation
- Hacking Tools
  - GetAdmin
  - hk.exe
- Keystroke Loggers
- Hacking Tools
  - IKS Software Keylogger
  - Ghost Keylogger
  - Hardware Key Logger
  - Spyware Spector
  - eBlaster

- Hiding Files
- Creating Alternate Data Streams
- ADS creation and detection
- Hacking Tools
  - Makestream
  - ads_cat
  - Streams
  - LADS (List Alternate Data Streams)
- NTFS Streams Countermeasures
- Stealing Files Using Word Documents
- Field Code Countermeasures
- Steganography
- Spyware Tool - Desktop Spy
- Hacking Tools
  - Steganography tools
    - DiSi-Steganograph
    - EZStego
    - Gif-It-Up v1.0
    - Gifshuffle
    - Hide and Seek
    - JPEG-JSTEG
    - MandelSteg and GIFExtract
    - Mp3Stego
    - Nicetext
    - Pretty Good Envelope
    - OutGuess
    - SecurEngine
    - Stealth
    - Snow
    - Steganography Tools 4
    - Steganos
    - Steghide
    - Stegodos
    - Stegonosaurus
    - StegonoWav
    - wbStego
  - Image Hide
  - MP3Stego
  - StegonoWav
  - Snow.exe
  - Camera/Shy
- Steganography Detection
- Hacking Tool

- diskprobe.exe
- Covering Tracks
- Disabling Auditing and clearing Event Logs
- Hacking Tool
  - Dump Event Log
  - elsave.exe
  - WinZapper
  - Evidence Eliminator
- RootKit
- Planting the NT/2000 RootKit
- Hacking Tools
  - Fu

    - Vanquish
- Rootkit Countermeasures
- Hacking Tool
    - Patchfinder 2.0

Class Section 5

Module 6: Trojans and Backdoors

- Effect on Business
- What is a Trojan?
- Overt and Covert Channels
- Working of Trojans
- Different Types of Trojans
- What Trojan Creators look for?
- Different ways a Trojan can get into a system
- Indications of a Trojan Attack
- Some famous Trojans and ports used by them
- How to determine which ports are "Listening"?
- Different Trojans found in the Wild
    - Beast 2.06
    - Phatbot
    - Senna Spy
    - CyberSpy
    - Remote Encrypted Callback UNIX Backdoor (RECUB)
    - Amitis
    - QAZ
    - Back Orifice
    - Back Orifice 2000
    - Tini
    - NetBus
    - SubSeven
    - Netcat
    - Subroot
    - Let me Rule 2.0 Beta 9
    - Donald Dick
    - Graffiti.exe
    - EliteWrap
    - IconPlus
    - Restorator
    - Whack-a-mole
    - Firekiller 2000
- BoSniffer
- Wrappers
- Packaging Tool : Wordpad
- Hard Disk Killer (HDKP 4.0)
- ICMP Tunneling
- Hacking Tool: Loki
- Loki Countermeasures
- Reverse WWW Shell – Covert Channels using HTTP
- Hacking Tools
    - fPort
    - TCP View

- Tripwire
- Process Viewer
- Inzider-Tracks Processes and Ports
- System File Verification
- Trojan horse Construction Kit
- Anti-Trojan
- Evading Anti-Trojan/Anti-Virus using Stealth Tools v 2.0
- Reverse Engineering Trojans
- Backdoor Countermeasures

Class Section 6

Module 7: Sniffers

- Definition of sniffing
- How a Sniffer works?
- Passive Sniffing
- Active Sniffing
- Hacking Tool: EtherFlood
- Man-in-the-Midle Attacks
- Spoofing and Sniffing Attacks
- ARP Poisoning and countermeasures
- Hacking Tools
  - Ethereal
  - Dsniff
  - Sniffit
  - Aldebaran
  - Hunt
  - NGSSniff
  - Ntop
  - pf
  - IPTraf
  - Etherape
  - Netfilter
  - Network Probe
  - Maa Tec Network Analyzer
  - Snort
  - Macof, MailSnarf, URLSnarf, WebSpy
  - Windump
  - Etherpeek
  - Ettercap
  - SMAC
  - Mac Changer
  - Iris
  - NetIntercept
  - WinDNSSpoof
  - NetIntercept
  - Win DNSpoof
  - TCPDump
  - Network Monitor
  - Gobbler
  - ETHLOAD
  - Esniff
  - Sunsniff
  - Linux_sniffer

- Sniffer Pro
- Sniffing Countermeasures

Class Section 7

Module 8: Denial of Service

- What is Denial of Service?
- Goal of DoS(Denial of Service)
- Impact and Modes of Attack
- DoS Attack Classification
  - Smurf
  - Buffer Overflow Attacks
  - Ping Of death
  - Teardrop
  - SYN
  - Tribal Flow Attack
- Hacking Tools
  - Jolt2
  - Bubonic.c
  - Land and LaTierra
  - Targa
- Distributed DOS Attacks and Characteristics
- Agent Handler Model
- IRC-Based DDoS Attack Model
- DDoS Attack taxonomy
- DDoS Tools
  - Trin00
  - Tribe Flow Network (TFN)
  - TFN2K
  - Stacheldraht
  - Shaft
  - Trinity
  - Knight
  - Mstream
  - Kaiten
- Reflected DOS Attacks
- Reflection of the Exploit
- Countermeasures for Reflected DoS
- Tools for Detecting DDOS Attacks
  - ipgrep
  - tcpdstat
  - findoffer
- DDoS Countermeasures
- Defensive Tool: Zombie Zapper
- Worms: Slammer and MyDoom.B

Module 9: Social Engineering

- What is Social Engineering?
- Art of Manipulation
- Human Weakness
- Common Types of Social Engineering
- Human Based Impersonation
- Example of social engineering
- Computer Based Social Engineering

- Reverse Social Engineering
- Policies and procedures
- Security Policies-checklist

Class Section 8

Module10: Session Hijacking

- Understanding Session Hijacking
- Spoofing vs Hijacking
- Steps in Session Hijacking
- Types of Session Hijacking
- TCP Concepts 3 Way Handshake
- Sequence numbers
- Hacking Tools
  - Juggernaut
  - T-Sight
  - TTY Watcher
  - IP Watcher
  - Hunt
  - Paros v3.1.1
  - TTY-Watcher
  - IP Watcher
  - T-sight
  - Remote TCP Session Reset Utility
- Dangers Posed by Session Hijacking
- Protection against Session Hijacking
- Countermeasures: IP Security

Module 11: Hacking Web Servers

- How Web Servers Work?
- How are Web Servers Compromised?
- Popular Web Servers and Common Security Threats
- Apache Vulnerability
- Attack against IIS
- IIS Components
- Sample Buffer Overflow Vulnerabilities
- Hacking Tool: IISHack.exe
- ISAPI.DLL Exploit
- Code Red and ISAPI.DLL Exploit
- Unicode
- Unicode Directory Traversal Vulnerability
- Hacking Tools
  - Unicodeuploader.pl
  - IISxploit.exe
  - execiis-win32.exe
- Msw 3prt IPP Vulnerability
- Hacking Tool: Jill.c
- IPP Buffer Overflow Countermeasures
- Unspecified Executed Path Vulnerability
- File System Traversal Countermeasures
- WebDAV/ ntdll.dll Vulnerability
- Real World instance of WebDAV Exploit

- Hacking Tool: “KaHT”
- RPCDCOM Vulnerability
- ASN Exploits
- IIS Logs
- Network Tool: Log Analyzer
- Hacking Tool: Clean IISLog
- Escalating Privileges on IIS
- Hacking Tools
  - hk.exe
  - cmdasp.asp
  - iiscrack.dll
  - ispc.exe
  - Microsoft IIS 5.0 - 5.1 remote denial of service Exploit Tool
  - Microsoft Frontpage Server Extensions fp30reg.dll Exploit Tool
  - GDI+ JPEG Remote Exploit Tool
  - Windows Task Scheduler Exploit Tool
  - Microsoft Windows POSIX Subsystem Local Privilege Escalation Exploit Tool
- Hot Fixes and Patches
- Solution: UpdateEXPERT
- cacls.exe Utility
- Vulnerability Scanners
- Network Tools
  - Whisker
  - N-Stealth
  - Webinspect
  - Shadow Security Scanner
- Countermeasures
- Increasing Web Server Security

Class Section 9

Module 12: Web Application Vulnerabilities

- Web Application Set-up
- Web Application Hacking
- Anatomy of an Attack
- Web Application Threats
- Cross Site Scripting/XSS Flaws
- An Example of XSS
- Countermeasures
- SQL Injection
- Command Injection Flaws
- Countermeasures
- Cookie/Session Poisoning
- Countermeasures
- Parameter/Form Tampering
- Buffer Overflow
- Countermeasures
- Directory Traversal/Forceful Browsing
- Countermeasures
- Cryptographic Interception
- Authentication Hijacking
- Countermeasures
- Log Tampering

        - Error Message Interception
        - Attack Obfuscation
        - Platform Exploits
        - Internet Explorer Exploits
        - DMZ Protocol Attacks
        - DMZ
        - Countermeasures
        - Security Management Exploits
        - Web Services Attacks
        - Zero Day Attacks
        - Network Access Attacks
        - TCP Fragmentation
        - Hacking Tools:
            - Instant Source
            - Wget
            - WebSleuth
            - Black Widow
            - Window Bomb
- Burp: Positioning Payloads
- Burp: Configuring Payloads and Content Enumeration
- Burp
- Burp Proxy: Intercepting HTTP/S Traffic
- Burp Proxy: Hex-editing of Intercepted Traffic
- Burp Proxy: Browser Access to Request History
- Hacking Tool: cURL
- Carnivore
- Google Hacking

Class Section 10

Module 13: Web Based Password Cracking Techniques

- Authentication- Definition
- Authentication Mechanisms
- HTTP Authentication
- Basic Authentication
- Digest Authentication
- Integrated Windows (NTLM) Authentication
- Negotiate Authentication
- Certificate-based Authentication
- Forms-based Authentication
- Microsoft Passport Authentication
- What is a Password Cracker?
- Modus Operandi of an Attacker using Password Cracker
- How does a Password Cracker work?
- Attacks- Classification
- Password Guessing
- Query String
- Cookies
- Dictionary Maker
- Password Crackers Available
    - LOphtcrack
    - John The Ripper
    - Brutus

    - Obiwan
    - Authforce
    - Hydra
    - Cain and Abel
    - RAR
    - Gammaprog
  - Hacking Tools:
    - WebCracker
    - Munga Bunga
    - PassList
    - Read Cookies
    - SnadBoy
    - WinSSLMiM
  - "Mary had a Little Lamb" Formula
  - Countermeasures

Module 14: SQL Injection

- Attacking SQL Servers
- SQL Server Resolution Service (SSRS)
- Osql-L Probing
- Port Scanning
- Sniffing, Brute Forcing and finding Application Configuration Files
- Tools for SQL Server Penetration Testing
  - SQLDict
  - SqlExec
  - SQLbf
  - SQLSmack
  - SQL2.exe
  - AppDetective
  - Database Scanner
  - SQLPoke
  - NGSSQLCrack
  - NGSSQuirreL
  - SQLPing v2.2
- OLE DB Errors
- Input Validation Attack
- Login Guessing & Insertion
- Shutting Down SQL Server
- Extended Stored Procedures
- SQL Server Talks
- Preventive Measures

Class Section 11

Module 15: Hacking Wireless Networks

- Introduction to Wireless Networking
- Business and Wireless Attacks
- Wireless Basics
- Components of Wireless Network
- Types of Wireless Network
- Setting up WLAN

- Detecting a Wireless Network
- How to access a WLAN
- Advantages and Disadvantages of Wireless Network
- Antennas
- SSIDs
- Access Point Positioning
- Rogue Access Points
- Tools to Generate Rogue Access Points
  - Fake AP
  - NetStumbler
  - MiniStumbler
- What is Wireless Equivalent Privacy (WEP)?
- WEP Tool:
  - AirSnort
  - WEPCrack
- Related Technology and Carrier Networks
- MAC Sniffing and AP Spoofing
- Tool to detect MAC Address Spoofing: Wellenreiter v2
- Terminology
- Denial of Service Attacks
- DoS Attack Tool: FATAjack
- Man-in-the-Middle Attack (MITM)
- Scanning Tools:
  - Redfang
  - Kismet
  - THC- WarDrive v2.1
  - PrismStumbler
  - MacStumbler
  - Mognet v1.16
  - WaveStumbler
  - StumbVerter v1.5
  - NetChaser v1.0 for Palm tops
  - AP Scanner
  - Wavemon
  - Wireless Security Auditor (WSA)
  - AirTraf 1.0
  - Wifi Finder
- Sniffing Tools:
  - AiroPeek
  - NAI Sniffer Wireless
  - Ethereal
  - Aerosol v0.65
  - vxSniffer
  - EtherPEG
  - Drifnet
  - AirMagnet
  - WinDump 3.8 Alpha
  - ssidsniff
- Multi Use Tool: THC-RUT
- Tool: WinPcap
- Auditing Tool: bsd-airtools
- WIDZ- Wireless Detection Intrusion System
- Securing Wireless Networks
- Out of the box Security
- Radius: Used as Additional layer in security
- Maximum Security: Add VPN to Wireless LAN

Class Section 12

Module 16 : Virus and Worms

- Virus Characteristics
- Symptoms of 'virus-like' attack
- What is a Virus Hoax?
- Terminologies
- How is a worm different from virus?
- Indications of a Virus Attack
- Virus History
- Virus damage
- Effect of Virus on Business
- Access Methods of a Virus
- Mode of Virus Infection
- Life Cycle of a virus
- What Virus Infect?
- How virus infect?
- Virus/worm found in the wild:
  - W32.CIH.Spacefiller (a.k.a Chernobyl)
  - Win32/Explore.Zip Virus
  - I Love You Virus
  - Melissa Virus
  - Pretty Park
  - Code red Worm
  - W32/Klez
  - Bug Bear
  - SirCam Worm
  - Nimda
  - SQL Slammer
- Writing a simple virus program.
- Writing DDOS Zombie Virus
- Virus Construction Kits
- Virus Creation Scripts
- Virus Detection Methods
- Virus Incident Response
- What is Sheep Dip?
- Prevention is better than Cure
- Anti-Virus Software
- Popular Anti-Virus packages
- New Virus found in 2004
- Virus Checkers
- Blaster – Virus Analysis
- Nimda – Virus Analysis
- Sasser Worm – Virus Analysis
- Klez – Virus Analysis
- IDAPro
- Virus Analyzers

Class Section 13

Module 17: Physical Security

- Security statistics
- Physical Security breach incidents
- Understanding Physical Security
- What is the need of Physical Security?
- Who is Accountable for Physical Security?
- Factors affecting Physical Security
- Physical Security checklist
  - Company surroundings
  - Premises
  - Reception
  - Server
  - Workstation Area
  - Wireless Access Points
  - Other Equipments such as fax, removable media etc
  - Access Control
  - Computer Equipment Maintenance
  - Wiretapping
  - Remote access
- Lock Picking Techniques
- Spying Technologies

Module 18: Linux Hacking

- Why Linux?
- Linux basics
- Chrooting
- Why is Linux Hacked?
- Linux Vulnerabilities in 2003
- How to apply patches to vulnerable programs
- Scanning Networks
- Scanning Tool: Nessus
- Cheops
- Port Scan detection tools:
  - Klaxon
  - Scanlogd
  - PortSentry
  - LIDS (Linux Intrusion Detection System)
- Password cracking in Linux.
- Password cracking tools:
  - John the Ripper
  - Viper
  - Slurpie
- IPChains
- IPTables
- ipchains vs. ipfwadm
- How to Organize Firewall Rules
- Security Auditor's Research Assistant (SARA)
- Hacking Tool:
  - Sniffit
  - HPing2

        - Hunt
        - TCP Wrappers
    - Linux Loadable Kernel Modules
    - Linux Rootkits:
        - Knark
        - Torn
        - Tuxit
        - Adore
        - Ramen
        - Beast
    - Rootkit countermeasures:
        - Chkrootki
        - Tripwire
        - Bastille Linux
        - LIDS(Linux Intrusion Detection system)
        - Dtk
        - Rkdet
        - Rootkit Hunter
        - Carbonite
        - Rscan
        - Saint Jude
    - Linux Security Tools:
        - Whisker
        - Flawfinder
    - Advanced Intrusion Detection System (AIDE)
    - Linux Security testing tools
        - NMap
        - LSOF
        - Netcat
        - Nemesis
- Linux Encryption Tools:
        - Stunnel
        - OpenSSH/SSH
        - SSH
        - GnuPG
    - Linux tools: Log and traffic monitors:
        - MRTG
        - Swatch
        - Timbersee
        - Logsurf
        - IPLog
        - IPTraf
        - Ntop
    - Linux Security Auditing Tool (LSAT)
    - Linux Security countermeasures

Class Section 14

Module 19: Evading Firewalls, IDS and Honeypots

- Intrusion Detection Systems
- Ways to Detect Intrusion
- Types of Intrusion Detection System
- Intrusion Detection Tools
  - Snort 2.1.0
  - Symantec ManHunt
  - LogIDS 1.0
  - SnoopNetCop Standard
  - Prelude Hybrid IDS version 0.8.x
  - Samhain
- Steps to perform after an IDS detects an intrusion
- Evading IDS systems
- Tools to Evade IDS
  - SideStep
  - ADMutate
  - Mendax v.0.7.1
  - Stick
  - Fragrouter
  - Anzen NIDSbench
- Packet Generators
- Introduction to Firewalls
- Firewall Identification
- Firewalking
- Banner Grabbing
- Breaching Firewalls
- Placing Backdoors through Firewalls
- Hiding Behind Covert Channel: Loki
- ACK tunneling
- Tools to Breach Firewall
  - 007 Shell
  - ICMP Shell
  - AckCmd
  - Covert TCP1.0
- Tools for testing IDS and Firewalls
- Introduction to Honeypots
- Honeypot Project
- Types of Honeypots
- Honeypot: Specter
- Honeypot: Honeyd
- Honeypot: KFSensor
- Hacking Tool: Sebek
- Tools to Detect Honeypot
  - Send-Safe Honeypot Hunter
  - Nessus Security Scanner

Module 20 : Buffer Overflows

- Significance of Buffer Overflow Vulnerability
- Why are Programs/Applications Vulnerable?

- Buffer Overflows
- Reasons for Buffer Overflow Attacks
- Knowledge required writing Buffer Overflow Exploits
- How a Buffer Overflow occurs?
- Understanding Stacks
- Stack Implementation
- Stack based buffer overflow
- Shellcode
- Heap Based buffer overflow
- How to detect Buffer Overflows in a Program?
- Attacking a real program
- NOPS
- How to mutate a Buffer Overflow Exploit? featuring ADMutate
- Countermeasures
- Return Address Defender (RAD)
- StackGuard
- Immunix System
- Vulnerability Search - ICAT

Class Section 15

Module 21 : Cryptography

- Public-key Cryptography
- Working of Encryption
- Digital Signature
- Digital Certificate
- RSA (Rivest Shamir Adleman)
- RSA Attacks
  - Brute forcing RSA factoring
  - Esoteric attack
  - Chosen cipher text attack
  - Low encryption exponent attack
  - Error analysis
  - Other attacks
- MD5
- SHA (Secure Hash Algorithm)
- SSL (Secure Socket Layer)
- RC5
- What is SSH?
- Government Access to Keys (GAK)
- RSA Challenge
- distributed.net
- PGP (Pretty Good Privacy)
- Code Breaking Methodologies
  - Using Brute Force
  - Frequency Analysis
  - Trickery and Deceit
  - One-Time Pad
- Cryptography Attacks
- Disk Encryption
- PGPCrack
- Magic Lantern
- WEPCrack
- Cracking S/MIME Encryption using idle CPU Time

- CypherCalc
- Command Line Scriptor
- CryptoHeaven

Module 22 : Penetration Testing

- Need for a Methodology
  - Penetration Test vs. Vulnerability Test
  - Reliance on Checklists and Templates
  - Phases of Penetration Testing
  - Passive Reconnaissance
  - Best Practices
  - Results that can be expected
  - Indicative passive reconnaissance steps include (but are not limited to)
  - Introduction to Penetration Testing
  - Type of Penetration Testing Methodologies
  - Open Source Vs Proprietary Methodologies
  - Security Assessment Vs Security Auditing
  - Risk Analysis
  - Types of Penetration Testing
  - Types Ethical Hacking
  - Vulnerability Assessment Vs Penetration Testing
  - Do-it Yourself Testing
  - Firms Offering Penetration Testing Services
  - Penetration Testing Insurance
  - Explication of Terms of Engagement
  - Pen-Test Service Level Agreements
  - Offer of Compensation
  - Starting Point and Ending Points of Testing
  - Penetration Testing Locations
  - Black Box Testing
  - White Box Testing
  - Grey Box Testing
  - Manual Penetration Testing
  - Automated Penetration Testing
  - Selecting the Right Tools
  - Pen Test Using Appscan
  - HackerShield
  - Pen-Test Using Cerberus Internet Scanner
  - Pen-Test Using CyberCop Scanner
  - Pen-Test Using Foundscan
  - Pen-Test Using Nessus
  - Pen-Test Using NetRecon
  - Pen-Test Using Retina
  - Pen-Test Using SAINT
  - Pen-Test Using SecureNET
  - Pen-Test Using SecureScan
  - Pen-Test Using SATAN, SARA and Security Analyzer
  - Pen-Test Using STAT Analyzer
  - Pen-Test Using Twwscan
  - VigilEnt
  - WebInspect
  - Evaluating Different Types of Pen-Test Tools
  - Platform on Which Tools Will be Used
  - Asset Audit

- Fault Tree and Attack Trees
- GAP Analysis
- Device Inventory
- Perimeter Firewall Inventory
- Web Server Inventory
- Load Balancer Inventory
- Local Area Network Inventory
- Demilitarized Zone Firewall
- Internal Switch Network Sniffer
- Application Server Inventory
- Database Server Inventory
- Name Controller and Domain Name Server
- Physical Security
- ISP Routers
- Legitimate Network Traffic Threat
- Unauthorized Network Traffic Threat
- Unauthorized Running Process Threat
- Loss of Confidential Information
- Business Impact of Threat
- Pre-testing Dependencies
- Post-testing Dependencies
- Failure Management
- Test Documentation Processes
- Penetration Testing Tools
    - Defect Tracking Tools
    - Configuration Management Tools
    - Disk Replication Tools
    - Pen-Test Project Scheduling Tools
    - Network Auditing Tools
    - DNS Zone Transfer Testing Tools
    - Trace Route Tools and Services
    - Network Sniffing Tools
    - Denial of Service Emulation Tools
    - Traditional Load Testing Tools
    - System Software Assessment Tools
    - Operating System Protection Tools
    - Fingerprinting Tools
    - Port Scanning Tools
    - Directory and File Access Control Tools
    - File Share Scanning Tools
    - Password Directories
    - Password Guessing Tools
    - Link Checking Tools
    - Web site Crawlers
    - Web-Testing based Scripting Tools
    - Buffer Overflow Protection Tools
    - Buffer Overflow Generation Tools
    - Input Data Validation Tools
    - File encryption Tools
    - Database Assessment Tools
    - Keyboard Logging and Screen Reordering Tools
    - System Event Logging and Reviewing Tools
    - Tripwire and Checksum Tools
    - Mobile-Code Scanning Tools
    - Centralized Security Monitoring Tools
    - Web Log Analysis Tools

        - Forensic Data and Collection Tools
        - Security Assessment Tools
        - Multiple OS Management Tools
    - SANS Institute TOP 20 Security Vulnerabilities
        - All Operating System Platforms
            - Default installs of operating systems and applications
            - Accounts with no passwords or weak passwords
            - Nonexistent or incomplete backups
            - Large number of open ports
            - Not filtering packets for correct incoming and outgoing addresses
            - Nonexistent or incomplete logging
            - Vulnerable Common Gateway Interface (CGI) programs
        - Windows-specific
            - Unicode vulnerability-Web server folder traversal
            - Internet server application programming interface (ISAPI) extension buffer overflows
            - IIS Remote Data Services (RDS) exploit
            - Network Basic Input Output System (NetBIOS), unprotected Windows networking shares
            - Information leakage via null session connections
            - Weak hashing in SAM (Security Accounts Manager)-LanManager hash
        - UNIX-specific
            - Buffer overflows in Remote Procedure Call (RPC) services
            - Sendmail vulnerabilities
            - Bind weaknesses
            - Remote system command (such as rcp, rlogin, and rsh) vulnerabilities
            - Line Printer Daemons (LPD) vulnerabilities
            - Sadmind and mountd exploits
            - Default Simple Network Management Protocol (SNMP) strings
    - Penetration Testing Deliverable Templates
        - Test Status Report Identifier
        - Test Variances
        - Test Comprehensive Assessment
        - Summary of Results (Incidents)
        - Test Evaluation
        - Names of Persons (Approval)
        - Template Test Incident Report
        - Template Test Log
    - Active Reconnaissance
    - Attack Phase
    - Activity: Perimeter Testing
    - Activity: Web Application Testing – I
    - Activity: Web Application Testing – II
    - Activity: Wireless Testing
    - Activity: Acquiring Target
    - Activity: Escalating Privileges
    - Activity: Execute, Implant & Retract
    - Post Attack Phase & Activities
    - Automated Penetration Testing Tool - CORE Impact