

H3X 3.1 LAB MANUAL

Module One – The Art of Hacking

Case study – IT Act 2000
Case study – Ethics and Culture
Discussion on approach of Hacking

Module Two – Scenario of Enterprise Security

Case Study – Infrastructure support of a company
Case Study – Skilled technical experts available
Discussion – Users Vs Administration
Case Study – Insider Trading
Discussion – Security Budget across different verticals
Discussion – Where is the Industry Heading?

Module Three - Planning and gathering Information

Technicalinfo.net
Netcraft.com
Godaddy.com
Domainsbyproxy
Forums
Social Networking - Myspace, orkut, facebook
Blogs - Technorati.com
Mouthshut.com
Job sites, Onesource.com
Plundering Local cyber cafe hard-drives
People search, Phone search
Archive.org
Paterva - Maltego project
Wikimapia.org - why its useful
Using google basic search techniques
Visual Route / Neo Trace
Email Tracker Pro
Nmap
Superscan
IPSecscan
User2Sid / Sid2User
NetBios Null Session
DumpSec
GFI Lan Guard Scanner
Organizing your thoughts – MindMapper Tool
Microsoft Visio

Module Four - Social Engineering

Case Study – Corporate Sabotage
Team Activity – Non Verbal Behavior
Team Activity – Blink Factor, Character Analysis
Team Activity - SMS and Chat psychology
Team Activity – Games people play

Module Five - Taking on the system

Using Group Policy Management Console
Windows Security configuration and Analysis tool
PGP – Using Encryption
L0pht Crack – Cracking the SAM
PwDump3
Using Keyloggers
Auto-start roots
Registry Hacking
Clearing Traces – deleting logs
Evidence Eliminator
Mac Address Spoofing
FakeGina
Resource Hacker
DCOM RPC Exploit
Privilege escalation tools
NTFS Streaming
Steganography – S-tools
Hiren Boot CD
Windows Live CD using BartPE

Module Six – Password Hacking

Hacking Active Directory Password
Advanced Password Recovery tools (Pdf, Zip, Office etc)
Using Brutus, Webcracker
Using Dictionaries
Using Rainbow tables
E-mail Hacking – Fake yahoo / MSN

Module 07 - Malwares, Rootkits and Trojans

Building a Trojan
Using NetBus, Subseven, Optix
Exe Binding tools
Adding white bytes to Trojans
Building Icons using Microangelo
Extracting Icons
Trojan Simulator
Analyzing a live Malware
Worm propagation tool
Melissa worm review
Vanquish Rootkit
Anti-spywares and Anti-viruses

Module 08 - Reality Hacking

Case Study – Influence of Occult in India
Case Study – Understanding Power of Religion across the world
Team Activity – Exploiting Religion and Occult science for Hacking
Team Activity – Bluffing as a Palmist and Astrologer
Team Activity – Games people Play (Transactional Analysis)

Module 09 – Getting Offensive

UDP Flooder
DDOS - Freak98
Smurf Attack
Email Bombers
Firewall Killer / Nuker
Using T-sight for Session Hijacking
Ethereal / Wireshark
Cane and Able
IIS 5.0 IPP, LSASS, Unicode Vulnerability
IIS Lock Down Tool

Module 10 - Web Application Hacking

Basic SQL, MySQL commands
Scanning for SQL Servers
Hacking a live website using SQL Injection
SQL password hacking tools – SQLbf, SQLDict
Advanced search techniques using Google
XSS Attacks – Live over Internet
Reflected and Stored XSS
Blog Hacking Concepts
Using Statcounter
Using Splogs for page ranking
Using MungaBunga, Brutus on Internet
Google Hacking – Search Techniques
SEO techniques and tools
Testing and installing Drupal on live server
Using PHPbb and getting overview of security
Firefox plugins: FireBug
Using Anonymizers
Hijack-This
Penetration Testing – Acunetix
Building a Fake site: Autophisher

Module 11 - Buffer Overflow & Rev Engineering

Buffer overflow – In depth Practical Lab
Using Win32Dasm for disassembling a file
Using HIEW for editing a file
Using OllyDbg for cracking
Using WinHex – lab for editing RAM
Monitoring Registry, Files, Disk Access, API using tools
Cracking a commercial application – 1 (Removing NAG screen)
Cracking a commercial application – 2 (Reversing Serial protection)
Cracking a commercial application – 3 (Time trial)
Creating a crack / patch for our cracked software
Protecting applications using Anti-debugging techniques etc.
Discussion – Cracking, Reversing Today

Module 12 - IDS, Firewalls and Forensics

Setting up snort – WinIDS pack
Setting up a Software Firewall
Activity: Crime scene analysis
MBR – Creation and backup
Recovering data from formatted hard-drives etc
Recovering data from CD, DVDs and other storage media
Sound Forensic Tools
Anti-Forensic Tools

Module 13 - Bluetooth and Wireless Security

Installing Bluetooth hacking tools on a mobile
Bluesnarfing attack on a vulnerable mobile
PDA security tools
Setting up an Ad-Hoc Wireless Network
Configuring an Access Point
Spoofing an Access Point
Using Kismet
Netstumbler
Using Airodump, AirCrack
Breaking WEP / WPA

Module 14 - VA & PT

Metasploit Framework
Ruby overview
Understanding exploit created in Ruby
MSF-XB introduction
Using Nessus
Generating Reports
Honeypots – KFSensor
HoneyBots, Trapservers
Log Analysis tools
Sending e-mail alerts for events
USB Security – USB Lock RP, DeviceLock
Print Censor

Module 15 - Patch Management and ISMS

Patch management
Risk Assessment Activity for a mock company
Threat Modeling
Conducting an Audit
Baseline Security Analyzer
Tools to audit for PCI-DSS
LanDesk overview
Evaluating Security Proposals
Activity: Faking as a security pre-sales guy
Activity: Seeking information from insiders
Activity: RFPs / Tenders
Case study on ISO 27001 best practices