CYBER SECURITY

SESSION 1-6

INTRODUCTION TO CYBER SECURITY

- Explaining the Certification, Introducing Security
- Introducing Hacking, Introduction to Ethical Hacking

FOOT PRINTING

- Defining Foot printing, Information Gathering Methodology
- Locate the Network Range, Hacking Tools

SCANNING

- Definition, Types, Objectives, Classification of Scanning
- Scanning Methodology, Hacking Tool, Countermeasures

ENUMERATION

- What is Enumeration? NetBios Null Sessions
- Hacking Tools, Enumerating User Accounts
- Active Directory Enumeration and Countermeasures

SYSTEM HACKING

- Administrator Password Guessing
- Manual Password Cracking Algorithm
- Automated Password Cracking, Password Types
- Types of Password Attacks, Hacking Tools

SESSION 7-12: TROJANS AND BACKDOORS

- Effect on Business, What is a Trojan?
- Overt and Covert Channels
- Indications of a Trojan Attack
- Reverse Engineering Trojans, Backdoor Countermeasures

SNIFFERS

- Definition of sniffing

- How a Sniffer works? Passive Sniffing
- Active Sniffing, Hacking Tools, Sniffing Countermeasures

DENIAL OF SERVICE

- What is Denial of Service?
- Goal of DoS (Denial of Service)
- Impact and Modes of Attack, DoS Attack Classification
- Hacking Tools, Countermeasures for Reflected DoS
- Tools for Detecting DDOS Attacks

SOCIAL ENGINEERING

- What is Social Engineering? Art of Manipulation
- Human Weakness, Common Types of Social Engineering
- Human Based Impersonation

SESSION HIJACKING

- Understanding Session Hijacking, Spoofing vs Hijacking
- Steps in Session Hijacking, Types of Session Hijacking
- Hacking Tools, Protection against Session Hijacking
- Countermeasures: IP Security

HACKING WEB SERVERS

- Popular Web Servers and Common Security Threats
- Apache Vulnerability, Attack against IIS Console
- Hacking Tools, Countermeasures
- Increasing Web Server Security

SESSION 13-20: WEB APPLICATION VULNERABILITIES

- Web Application Hacking, Anatomy of an Attack
- Web Application Threats, Carnivore, Google Hacking
- Countermeasures

WEB BASED PASSWORD CRACKING TECHNIQUES

- Authentication- Definition, Authentication Mechanisms
- Password Guessing, Query String, Cookies
- Password Crackers Available
- Hacking Tools, Countermeasures

SQL INJECTION

- Attacking SQL Servers, SQL Server Resolution Service
- Osql-L Probing, Port Scanning, SQL Server Talks
- Preventive Measures

HACKING WIRELESS NETWORKS

- Wireless Basics, Components of Wireless Network
- Access Point Positioning, Rogue Access Points
- Tools to Generate Rogue Access Points
- Scanning Tools, Sniffing Tools
- Securing Wireless Networks

WORMS AND VIRUSES

- Virus Characteristics, Symptoms of 'virus-like' attack
- Indications of a Virus Attack
- Virus / Worms found in the wild
- Virus writing tools, Virus Checkers, Virus Analyzers

PHYSICAL SECURITY

- Understanding & Factors Affecting Physical Security
- Wiretapping, Lock Picking Techniques
- Spying Technologies

LINUX HACKING

- Linux Basics, Linux Vulnerabilities, Scanning Networks

- Scanning & Linux Security Tools
- Adv. Intrusion Detection System
- Linux Security Auditing Tool
- Linux Security Countermeasures

EVADING FIREWALLS, IDS AND HONEYPOTS

- Intrusion Detection Systems, Ways to Detect Intrusion
- Types of Intrusion Detection System
- Intrusion Detection Tools
- Honeypot Project, Tools to Detect Honeypot

BUFFER OVERFLOWS

- Buffer Overflows, How a Buffer Overflow Occurs
- Shellcode, NOPS, Countermeasures

SESSION 21-32: PENETRATION TESTING

- Introduction to Penetration Testing (PT)
- Categories of security assessments
- Vulnerability Assessment
- Limitations of Vulnerability Assessment, Testing
- Penetration Testing Tools, Threat
- Other Tools Useful in Pen-Test
- Phases of Penetration Testing
- Post Attack Phase and Activities
- Penetration Testing Deliverables Templates

COVERT HACKING

- Insider Attacks, What is Covert Channel?
- Security Breach
- Why Do You Want to Use Covert Channel?
- Motivation of a Firewall Bypass, Covert Channels Scope

- Covert Channel: Attack Techniques
- Simple Covert Attacks
- Advanced Covert Attacks, Standard Direct Connection
- Reverse Shell (Reverse Telnet)

WRITING VIRUS CODES

- Introduction of Virus, Types of Viruses
- Symptoms of a Virus Attack
- Prerequisites for Writing Viruses
- Required Tools and Utilities, Virus Infection Flow Chart
- Components of Viruses, Testing Virus Codes
- Tips for Better Virus Writing

EXPLOIT WRITING

- Exploits Overview, Purpose of Exploit Writing
- Prerequisites for Writing Exploits and Shellcodes
- Types of Exploits, Stack Overflow, Heap Corruption
- The Proof-of-Concept and Commercial Grade Exploit
- Converting a Proof of Concept Exploit to Commercial Grade
- Attack Methodologies, Socket Binding Exploits
- Tools for Exploit Writing, Steps for Writing an Exploit
- Difference Between Windows & Linux Exploit, Shellcode
- NULL Byte, Types of Shellcodes
- Steps for Writing a Shellcode
- Tools Used for Shellcode Development
- Issues Involved With Shellcode Writing

SMASHING THE STACK FOR FUN AND PROFIT

- What is a Buffer? Static Vs Dynamic Variables

- Stack Buffers, Data Region, Memory Process Regions
- What Is A Stack? Why Do We Use A Stack?
- The Stack Region, Stack frame, Stack pointer
- Procedure Call, Compiling the code to assembly
- Call Statement, Return Address (RET), Word Size, Stack
- Buffer Overflows
- Why do we get a segmentation violation?
- Segmentation Error, Instruction Jump
- Guess Key Parameters, Calculation, Shell Code

SESSION 33-40: WINDOWS BASED BUFFER OVERFLOW EXPLOIT WRITING

- Buffer & Stack overflow
- Writing Windows Based Exploits
- Exploiting stack based buffer overflow
- OpenDataSource Buffer Overflow Vulnerability Details
- Simple Proof of Concept, Windbg.exe
- Analysis, EIP Register
- Execution Flow, But where can we jump to?
- Offset Address, The Query, Finding jmp esp
- Debug.exe, listdlls.exe, Msvcrt.dll, Out.sql, The payload
- ESP, Limited Space, Memory Address
- Getting Windows API/function absolute address
- Other Addresses, Compile the program, Final Code

REVERSE ENGINEERING

- Positive Applications of Reverse Engineering
- Ethical Reverse Engineering, World War Case Study
- DMCA Act, What is Disassembler?
- Why do you need to decompile?
- Professional Disassembler Tools, Decompilers

- Program Obfuscation
- Convert Assembly Code to C++ code
- Machine Decompilers

HACKING ROUTERS, CABLE MODEMS AND FIREWALLS

- Network Devices, Identifying a Router
- HTTP Configuration Arbitrary Administrative Access Vulnerability, ADMsnmp, Solarwinds MIB Browser
- Brute-Forcing Login Services, Hydra
- Analyzing the Router Config
- Cracking the Enable Password
- Tool: Cain and Abel, Implications of a Router Attack
- Types of Router Attacks, Router Attack Topology
- Denial of Service (DoS) Attacks
- Packet “Mistreating” Attacks
- Cisco Router, Eigrp-tool, Tool: Zebra
- Tool: Yersinia for HSRP, CDP, and other layer 2 attacks
- Tool: Cisco Torch, Monitoring SMTP (port25) Using SLcheck
- Monitoring HTTP(port 80) Cable Modem Hacking

HACKING MOBILE PHONES, PDA AND HANDHELD DEVICES

- Different OS in Mobile Phone
- Different OS Structure in Mobile Phone
- Evolution of Mobile Threat, What Can A Hacker Do
- Vulnerabilities in Different Mobile Phones, Malware
- Spyware, Blackberry, PDA, iPod, Viruses, Antivirus
- Mobile: Is It a Breach to Enterprise Security?
- Security Tools, Defending Cell Phones and PDAs Against Attack, Mobile Phone Security Tips

BLUETOOTH HACKING

- Bluetooth Introduction, Security Issues in Bluetooth

- Security Attacks in Bluetooth Devices
- Bluetooth hacking tools, Bluetooth Viruses and Worms
- Bluetooth Security tools, Countermeasures

VOIP HACKING

- What is VoIP, VoIP Hacking Step, Footprinting
- Scanning, Enumeration, Steps to Exploit the Network
- Covering Tracks

SPAMMING

- Techniques used by Spammers
- How Spamming is performed
- Ways of Spamming, Statistics, Worsen ISP: Statistics
- Top Spam Effected Countries: Statistics
- Type of Spam Attacks, Spamming Tool
- Anti-Spam Techniques, Anti- Spamming Tool
- Countermeasures

SESSION 41-50: GOOGLE HACKING

- What is Google hacking
- What a hacker can do with vulnerable site
- Anonymity with Caches, Using Google as a Proxy Server
- Traversal Techniques, Extension Walking, Site Operator
- Locating Public Exploit Sites
- Locating Vulnerable Targets
- Directory Listings, Web Server Software Error Messages
- Application Software Error Messages, Default Pages
- Searching for Passwords

HACKING EMAIL ACCOUNTS

- Ways of Getting Email Account Information

- Vulnerabilities
- Email Hacking Tools, Securing Email Accounts

CRYPTOGRAPHY

- Public-key Cryptography, Working of Encryption
- Digital Signature, RSA (Rivest Shamir Adleman)
- RC4, RC5, RC6, Blowfish, Algorithms and Security
- Brute-Force Attack, RSA Attacks
- Message Digest Functions
- SHA (Secure Hash Algorithm) SSL (Secure Sockets Layer)
- What is SSH, Government Access to Keys (GAK) RSA Challenge, Distributed.net, Code Breaking: Methodologies
- Cryptography Attacks, Disk Encryption, Magic Lantern
- WEPCrack, Cracking S/MIME Encryption Using Idle CPU Time

RFID HACKING

- Components of RFID Systems, RFID Collision, RFID Risks

HACKING USB DEVICES

- Electrical, Software, USB Attack on Windows
- Viruses & Worm
- Hacking Tools, USB Security Tools, Countermeasures

HACKING DATABASE SERVERS

- Hacking Oracle Database Server & SQL Server
- Security Tools
- SQL Server Security Best Practices: Administrator and Developer Checklists

INTERNET CONTENT FILTERING TECHNIQUES

- Introduction to Internet Filter
- Key Features of Internet Filters

- Pros & Cons of Internet Filters
- Internet Content Filtering Tool
- Internet Safety Guidelines for Children

SESSION 51-60: PRIVACY ON THE INTERNET

- Internet, Proxy, Spyware, Email privacy, Cookies
- Examining Information in Cookies
- How Internet Cookies Work
- How Google Stores Personal Information
- Google Privacy Policy, Web Browsers, Web Bugs
- Downloading Freeware, Internet Relay Chat
- Pros and Cons of Internet Relay Chat
- Electronic Commerce
- Internet Privacy Tools: Anonymizers, Firewall Tools
- Best Practices, Counter measures

SECURING LAPTOP COMPUTERS

- Statistics for Stolen & Recovered Laptops
- Statistics on Security
- Percentage of Organization Following the Security Measures, Laptop threats, Laptop Theft
- Fingerprint Reader
- Protecting Laptops Through Face Recognition
- Bluetooth in Laptops
- Securing from Physical Laptop Thefts
- Hardware Security for Laptops
- Protecting the Sensitive Data
- Preventing Laptop Communications from Wireless Threats, Security Tips
- Protecting the Stolen Laptops from Being Used

CREATING SECURITY POLICIES

- Security policies, Key Elements of Security Policy
- Defining the Purpose and Goals of Security Policy
- Role of Security Policy, Classification of Security Policy
- Design of Security Policy, Contents of Security Policy
- Configurations & Implementing Security Policies
- Types of Security Policies, Policy Statements
- Basic Document Set of Information Security Policies
- E-mail, Software Security & Software License Policy
- Points to Remember While Writing a Security Policy

SOFTWARE PIRACY AND WAREZ

- Process of Software Activation, Piracy
- Software Copy Protection Backgrounders
- Warez, Tools

HACKING WEB BROWSERS

- How Web Browsers Work
- How Web Browsers Access HTML Documents
- Protocols for an URL, Hacking Firefox, Firefox Security
- Hacking Internet Explorer, Internet Explorer Security
- Hacking Opera, Security Features of Opera
- Hacking & Securing Safari, Hacking & Securing Netscape

PROXY SERVER TECHNOLOGIES

- Working of Proxy Server, Types of Proxy Server
- Socks Proxy, Free Proxy Servers
- Use of Proxies for Attack, How Does MultiProxy Work
- TOR Proxy Chaining Software, AnalogX Proxy, NetProxy
- Proxy+, ProxySwitcher Lite, Tool: JAP, Proxomitron
- SSL Proxy Tool, How to Run SSL Proxy

DATA LOSS PREVENTION

- Causes of Data Loss, How to Prevent Data Loss
- Impact Assessment for Data Loss Prevention, Tools

COMPUTER FORENSICS AND INCIDENT HANDLING

- Computer Forensics, What is Computer Forensics
- Need for Computer Forensics
- Objectives of Computer Forensics
- Stages of Forensic Investigation in Tracking Cyber Criminals
- Key Steps in Forensic Investigations
- List of Computer Forensics Tools, Incident Handling

Incident Management

- Why don't Organizations Report Computer Crimes
- Estimating Cost of an Incident
- Whom to Report an Incident, Incident Reporting
- Vulnerability Resources, CSIRT: Goals and Strategy

FIREWALL TECHNOLOGIES

- Hardware and Software Firewalls
- Windows & Mac OS X Firewalls