

EC-Council Certified Network Defense Architect (CNDA)

Course Summary

Description

This class will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking.

This course prepares you for Certified Network Defense Architect exam 312-99

Topics

- Ethics and Legality
- Footprinting
- Scanning
- Enumeration
- System Hacking
- Trojans & Backdoors
- Sniffers
- Denial of Service
- Social Engineering
- Session Hijacking
- Hacking Web Servers
- Web Application Vulnerabilities
- Web Based Password Cracking Techniques
- SQL injection
- Hacking Wireless Networks
- Virus and Worms
- Physical Security
- Linux Hacking
- Evading Firewalls, IDS and Honeypots
- Buffer Overflows
- Cryptography
- Penetration Testing

Audience

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. This course was specially designed for Government Agencies.

Prerequisites

There are no prerequisites for this course.

Duration

Five days

EC-Council Certified Network Defense Architect (CNDA)**Course Outline**

- I. Ethics and Legality**
 - A. Why Security?
 - B. The Security, functionality and ease of use Triangle
 - C. Can Hacking be Ethical?
 - D. Essential Terminology.
 - E. Elements of Security.
 - F. What does a Malicious Hacker do?
 - G. Difference between Penetration Testing and Ethical Hacking.
 - H. Hacker Classes.
 - I. What do Ethical Hackers do?
 - J. Skill Profile of an Ethical Hacker.
 - K. Modes of Ethical Hacking.
 - L. Security Testing.
 - M. Deliverables.
 - N. Computer Crimes and Implications.
 - O. Legal Perspective (US Federal Laws).
 - II. Footprinting**
 - A. Defining Footprinting.
 - B. Information Gathering Methodology.
 - C. Locate the Network Range.
 - D. Hacking Tools:
 - 1. Whois
 - 2. Nslookup
 - 3. ARIN
 - 4. Traceroute
 - 5. NeoTrace
 - 6. VisualRoute Trace
 - 7. SmartWhois
 - 8. Visual Lookout
 - 9. VisualRoute Mail Tracker
 - 10. eMailTrackerPro
 - III. Scanning**
 - A. Definition of Scanning.
 - B. Types of scanning
 - C. Objectives of Scanning
 - D. Scanning Methodology
 - E. Classification of Scanning
 - F. Hacking Tools
 - 1. Nmap
 - 2. XMAS Scan
 - 3. FIN Scan
 - 4. Null Scan
 - 5. Windows Scan
 - 6. Idle Scan
 - 7. Nessus
 - 8. Retina
 - 9. Saint
 - IV. Enumeration**
 - A. What is Enumeration?
 - B. NetBios Null Sessions
 - C. Hacking Tools
 - 1. DumpSec
 - 2. Winfo
 - 3. NetBIOS Auditing Tool (NAT)
 - D. Null Session Countermeasures
 - E. NetBIOS Enumeration
 - F. Hacking Tool :NBTScan
 - G. Simple Network Management
 - 1. Protocol (SNMP) Enumeration
 - H. Hacking Tools
 - 1. Solarwinds
 - 2. Enum
 - I. SNScan
- 10. HPing2
 - 11. Firewall
 - 12. NIKTO
 - 13. GFI Languard
 - 14. ISS Security Scanner
 - 15. Netcraft
 - 16. IPsec Scan
 - 17. NetScan Tools pro 2003
 - 18. Super Scan
 - 19. Floppyscan
 - G. War Dialer
 - H. Hacking Tools
 - 1. THC Scan
 - 2. Friendly Pinger
 - 3. Cheops
 - 4. Security Administrator's Tool for Analyzing Network (SATAN)
 - 5. SAFEsuite Internet Scanner
 - 6. IdentTCPScan
 - 7. PortScan Plus
 - 8. Strobe
 - 9. Blaster Scan
 - I. OS Fingerprinting
 - J. Active Stack fingerprinting
 - K. Tool for Active Stack fingerprinting
 - 1. XPROBE2
 - L. Passive Fingerprinting
 - M. Proxy Servers
 - N. Hacking Tools
 - 1. Socks Chain
 - 2. Anonymizers
 - 3. HTTP Tunnel
 - 4. HTTPort
 - O. Countermeasures

EC-Council Certified Network Defense Architect (CNDA)**Course Outline (con't)**

- J. SNMP Enumeration Countermeasures
- K. Management Information Base (MIB)
- L. Windows 2000 DNS Zone Transfer
- M. Blocking Win 2k DNS Zone Transfer
- N. Enumerating User Accounts
- O. Hacking Tools
 - 1. User2sid and Sid2user
 - 2. UserInfo
 - 3. GetAcct
 - 4. DumpReg
 - 5. Trout
 - 6. Winfingerprint
 - 7. PsTools
 - 8. (PSFile,PSLoggedOn,PSGetSid,PSInfo,PSService,P SList,PSKill, PSSuspend, PSLogList, PSExec, PSShutdown)
- P. Active Directory Enumeration and Countermeasures
- V. System Hacking**
 - A. Administrator Password Guessing
 - B. Manual Password Cracking Algorithm
 - C. Automated Password Cracking
 - D. Password Types
 - E. Types of Password Attacks
 - F. Hacking Tool
 - 1. NTInfoScan (CIS)
 - G. Performing Automated Password Guessing
 - H. Hacking Tool
 - I. Legion
 - J. Password Sniffing
 - K. Hacking Tools
 - 1. LOphcrack
 - 2. pwdump2 and pwdump3
 - 3. KerbCrack
 - 4. NBTdeputy
 - L. NetBIOS DoS Attack
 - M. Hacking Tools
 - 1. NBName
 - 2. John the Ripper
 - N. LAN Manager Hash
 - O. Password Cracking Countermeasures
 - P. Syskey Utility
 - Q. Cracking NT/2000 Passwords
 - R. Hacking Tool
 - 1. NTFSDOS
 - S. SMB Logon
 - T. Hacking Tool: SMBRelay
 - U. SMBRelay Man-in-the-Middle Scenario
 - V. Hacking Tool : SMBRelay2
 - W. SMBRelay Weaknesses and Countermeasures
 - X. Hacking Tools
 - 1. SMBGrind
 - 2. SMBDie
 - Y. Privilege Escalation
 - Z. Hacking Tools
 - 1. GetAdmin
 - 2. hk.exe
 - AA. Keystroke Loggers
 - BB. Hacking Tools
 - 1. IKS Software Keylogger
 - 2. Ghost Keylogger
 - 3. Hardware Key Logger
 - 4. Spyware Spector
 - 5. eBlaster
 - CC. Hiding Files
 - DD. Creating Alternate Data Streams
 - EE. ADS creation and detection
 - FF. Hacking Tools
 - 1. Makestream
 - 2. ads_cat
 - 3. Streams
 - 4. LADS (List Alternate Data Streams)
 - GG. NTFS Streams Countermeasures
 - HH. Stealing Files Using Word Documents
 - II. Field Code Countermeasures
 - JJ. Steganography
 - KK. Spyware Tool - Desktop Spy
 - LL. Hacking Tools
 - 1. Steganography tools
 - A. DiSi-Steganograph
 - B. EZStego
 - C. Gif-It-Up v1.0 Gifshuffle
 - D. Hide and Seek JPEG-JSTEG MandelSteg and GIFExtract Mp3Stego
 - E. Nicetext
 - F. Pretty Good Envelope
 - G. OutGuess
 - H. SecurEngine
 - I. Stealth
 - J. Steganos
 - K. Steghide
 - L. Stegodos
 - M. Stegonosaurus
 - N. StegonoWav
 - O. wbStego
 - 2. Image Hide
 - 3. MP3Stego
 - 4. StegonoWav
 - 5. Snow.exe

EC-Council Certified Network Defense Architect (CNDA)

Course Outline (con't)

- 6. Camera/Shy
 - MM. Steganography Detection
 - NN. Hacking Tool
 - 1. diskprobe.exe
 - OO. Covering Tracks
 - PP. Disabling Auditing and clearing Event Logs
 - QQ. Hacking Tool
 - 1. Dump Event Log
 - 2. elsave.exe
 - 3. WinZapper
 - 4. Evidence Eliminator
 - RR. RootKit
 - SS. Planting the NT/2000 RootKit
 - TT. Hacking Tools
 - 1. Fu
 - 2. Vanquish
 - UU. Rootkit Countermeasures
 - VV. Hacking Tool
 - 1. Patchfinder 2.0
- VI. Trojans and Backdoors**
- A. Effect on Business
 - B. What is a Trojan?
 - C. Overt and Covert Channels
 - D. Working of Trojans
 - E. Different Types of Trojans
 - F. What Trojan Creators look for?
 - G. Different ways a Trojan can get into a system
 - H. Indications of a Trojan Attack
 - I. Some famous Trojans and ports used by them
 - J. How to determine which ports are "Listening"?
 - K. Different Trojans found in the Wild
 - 1. Beast 2.06
 - 2. Phatbot
 - 3. Senna Spy
 - 4. CyberSpy
 - 5. Remote Encrypted Callback UNIX Backdoor (RECUB)
 - 6. Amitis
 - 7. QAZ
 - 8. Back Orifice
 - 9. Back Orifice 2000
 - 10. Tini
 - 11. NetBus
 - 12. SubSeven
 - 13. Netcat
 - 14. Subroot
 - 15. Let me Rule 2.0 Beta 9
- 16. Donald Dick
 - 17. Graffiti.exe
 - 18. EliteWrap
 - 19. IconPlus
 - 20. Restorator
 - 21. Whack-a-mole
 - 22. Firekiller 2000
 - L. BoSniffer
 - M. Wrappers
 - N. Packaging Tool : Wordpad
 - O. Hard Disk Killer (HDKP 4.0)
 - P. ICMP Tunneling
 - Q. Hacking Tool: Loki
 - R. Loki Countermeasures
 - S. Reverse WWW Shell – Covert Channels using HTTP
 - T. Hacking Tools
 - 1. fPort
 - 2. TCP View
 - U. Tripwire
 - V. Process Viewer
 - W. Inzider-Tracks Processes and Ports
 - X. System File Verification
 - Y. Trojan horse Construction Kit
 - Z. Anti-Trojan
 - AA. Evading Anti-Trojan/Anti-Virus using Stealth Tools v 2.0
 - BB. Reverse Engineering Trojans
 - CC. Backdoor Countermeasures
- VII. Sniffers**
- A. Definition of sniffing
 - B. How a Sniffer works?
 - C. Passive Sniffing
 - D. Active Sniffing
 - E. Hacking Tool: EtherFlood
 - F. Man-in-the-Middle Attacks
 - G. Spoofing and Sniffing Attacks
 - H. ARP Poisoning and countermeasures
 - 1. Hacking Tools
 - 2. Ethereal
 - 3. Dsniff
 - 4. Sniffit
 - 5. Aldebaran
 - 6. Hunt
 - 7. NGSSniff
 - 8. Ntop pf
 - 9. IPTraf Etherape Netfilter Network Probe
 - 10. Windump
 - 11. Etherpeek
 - 12. Ettercap

EC-Council Certified Network Defense Architect (CNDA)

Course Outline (con't)

- 13. SMAC
 - 14. Mac Changer
 - 15. Iris
 - 16. NetIntercept
 - 17. WinDNSSpoof
 - 18. NetIntercept
 - 19. Win DNSpoof
 - 20. TCPDump
 - 21. Network Monitor
 - 22. Gobbler
 - 23. ETHLOAD
 - 24. Esniff
 - 25. Sunsniff
 - 26. Linux_sniffer
 - 27. Sniffer Pro
- I. Sniffing Countermeasures
- VIII. Denial of Service**
- A. What is Denial of Service?
 - B. Goal of DoS(Denial of Service)
 - C. Impact and Modes of Attack
 - D. DoS Attack Classification
 - 1. Smurf
 - 2. Buffer Overflow Attacks
 - 3. Ping Of death
 - 4. Teardrop
 - 5. SYN
 - 6. Tribal Flow Attack
 - E. Hacking Tools
 - 1. Jolt2
 - 2. Bubonic.c
 - 3. Land and LaTierra
 - 4. Targa
 - F. Distributed DOS Attacks and Characteristics
 - G. Agent Handler Model
 - H. IRC-Based DDoS Attack Model
 - I. DDoS Attack taxonomy
 - J. DDoS Tools
 - 1. Trin00
 - 2. Tribe Flow Network (TFN)
 - 3. TFN2K Stacheldraht Shaft Trinity Knight
 - 4. Mstream
 - 5. Kaiten
 - K. Reflected DOS Attacks
 - L. Reflection of the Exploit
 - M. Countermeasures for Reflected DoS
 - N. Tools for Detecting DDOS Attacks
 - 1. ipgrep
 - 2. tcpdstat
 - 3. findoffer
 - O. DDoS Countermeasures
 - P. Defensive Tool: Zombie Zapper
 - Q. Worms: Slammer and MyDoom.B
- IX. Social Engineering**
- A. What is Social Engineering?
 - B. Art of Manipulation
 - C. Human Weakness
 - D. Common Types of Social Engineering
 - E. Human Based Impersonation
 - F. Example of social engineering
 - G. Computer Based Social Engineering
 - H. Reverse Social Engineering
 - I. Policies and procedures
 - J. Security Policies-checklist
- X. Session Hijacking**
- A. Understanding Session Hijacking
 - B. Spoofing vs Hijacking
 - C. Steps in Session Hijacking
 - D. Types of Session Hijacking
 - E. TCP Concepts 3 Way Handshake
 - F. Sequence numbers
 - G. Hacking Tools
 - 1. Juggernaut
 - 2. T-Sight
 - 3. TTY Watcher
 - 4. IP Watcher
 - 5. Hunt
 - 6. Paros v3.1.1
 - 7. TTY-Watcher
 - 8. IP Watcher
 - 9. T-sight
 - 10. Remote TCP Session Reset Utility
 - H. Dangers Posed by Session Hijacking
 - I. Protection against Session Hijacking
 - J. Countermeasures: IP Security
- XI. Hacking Web Servers**
- A. How Web Servers Work?
 - B. How are Web Servers Compromised?
 - C. Popular Web Servers and Common Security Threats
 - D. Apache Vulnerability
 - E. Attack against IIS
 - F. IIS Components
 - G. Sample Buffer Overflow Vulnerabilities
 - H. Hacking Tool: IISHack.exe
 - I. ISAPI.DLL Exploit
 - J. Code Red and ISAPI.DLL Exploit
 - K. Unicode
 - L. Unicode Directory Traversal Vulnerability

EC-Council Certified Network Defense Architect (CNDA)**Course Outline (con't)**

- M. Hacking Tools
 - 1. Unicodeuploader.pl
 - 2. IISxploit.exe
 - 3. execiis-win32.exe
 - N. Msw 3prt IPP Vulnerability
 - O. Hacking Tool: Jill.c
 - P. IPP Buffer Overflow Countermeasures
 - Q. Unspecified Executed Path Vulnerability
 - R. File System Traversal Countermeasures
 - S. WebDAV/ ntdll.dll Vulnerability
 - T. Real World instance of WebDAV Exploit
 - U. Hacking Tool: "KaHT"
 - V. RPCDCOM Vulnerability
 - W. ASN Exploits
 - X. IIS Logs
 - Y. Network Tool: Log Analyzer
 - Z. Hacking Tool: Clean IISLog
 - AA. Escalating Privileges on IIS
 - BB. Hacking Tools
 - 1. hk.exe
 - 2. cmdasp.asp
 - 3. iiscrack.dll
 - 4. ispc.exe
 - 5. Microsoft IIS 5.0 - 5.1 remote denial of service Exploit Tool
 - 6. Microsoft Frontpage Server Extensions fp30reg.dll Exploit Tool
 - 7. =GDI+ JPEG Remote Exploit Tool
 - 8. Windows Task Scheduler Exploit Tool
 - 9. Microsoft Windows POSIX Subsystem Local Privilege Escalation Exploit Tool
 - CC. Hot Fixes and Patches
 - DD. Solution: UpdateEXPERT
 - EE. cacls.exe Utility
 - FF. Vulnerability Scanners
 - GG. Network Tools
 - 1. Whisker
 - 2. N-Stealth
 - 3. Webinspect
 - 4. Shadow Security Scanner
 - HH. Countermeasures
 - II. Increasing Web Server Security
- XII. Web Application Vulnerabilities**
- A. Web Application Set-up
 - B. Web Application Hacking
 - C. Anatomy of an Attack
 - D. Web Application Threats
 - E. Cross Site Scripting/XSS Flaws
 - F. An Example of XSS
- G. Countermeasures
 - H. SQL Injection
 - I. Command Injection Flaws
 - J. Countermeasures
 - K. Cookie/Session Poisoning
 - L. Countermeasures
 - M. Parameter/Form Tampering
 - N. Buffer Overflow
 - O. Countermeasures
 - P. Directory Traversal/Forceful Browsing
 - Q. Countermeasures
 - R. Cryptographic Interception
 - S. Authentication Hijacking
 - T. Countermeasures
 - U. Log Tampering
 - V. Error Message Interception
 - W. Attack Obfuscation
 - X. Platform Exploits
 - Y. Internet Explorer Exploits
 - Z. DMZ Protocol Attacks
 - AA. DMZ
 - BB. Countermeasures
 - CC. Security Management Exploits
 - DD. Web Services Attacks
 - EE. Zero Day Attacks
 - FF. Network Access Attacks
 - GG. TCP Fragmentation
 - HH. Hacking Tools:
 - 1. Instant Source
 - 2. Wget
 - 3. WebSleuth
 - 4. Black Widow
 - 5. Window Bomb
 - II. Burp: Positioning Payloads
 - JJ. Burp: Configuring Payloads and Content Enumeration
 - KK. Burp
 - LL. Burp Proxy: Intercepting HTTP/S Traffic
 - MM. Burp Proxy: Hex-editing of Intercepted Traffic
 - NN. Burp Proxy: Browser Access to Request History
 - OO. Hacking Tool: cURL
 - PP. Carnivore
 - QQ. Google Hacking
- XIII. Web Based Password Cracking Techniques**
- A. Authentication- Definition
 - B. Authentication Mechanisms
 - C. HTTP Authentication
 - D. Basic Authentication
 - E. Digest Authentication

EC-Council Certified Network Defense Architect (CNDA)

Course Outline (con't)

- F. Integrated Windows (NTLM) Authentication
- G. Negotiate Authentication
- H. Certificate-based Authentication
- I. Forms-based Authentication
- J. Microsoft Passport Authentication
- K. What is a Password Cracker?
- L. Modus Operandi of an Attacker using Password Cracker
- M. How does a Password Cracker work?
- N. Attacks- Classification
- O. Password Guessing
- P. Query String
- Q. Cookies
- R. Dictionary Maker
- S. Password Crackers Available
 - 1. LOphcrack
 - 2. John The Ripper
 - 3. Brutus
 - 4. Obiwan
 - 5. Authforce
 - 6. Hydra
 - 7. Cain and Abel
 - 8. RAR
 - 9. Gammalog
- T. Hacking Tools:
 - 1. WebCracker
 - 2. Munga Bunga
 - 3. PassList
 - 4. Read Cookies
 - 5. SnadBoy
 - 6. WinSSLMIM
- U. "Mary had a Little Lamb" Formula
- V. Countermeasures

XIV. SQL Injection

- A. Attacking SQL Servers
- B. SQL Server Resolution Service (SSRS)
- C. Osql-L Probing
- D. Port Scanning
- E. Sniffing, Brute Forcing and finding Application Configuration Files
- F. Tools for SQL Server Penetration Testing
 - 1. SQLDict
 - 2. SqlExec
 - 3. SQLbf
 - 4. SQLSmack
 - 5. SQL2.exe
 - 6. AppDetective
 - 7. Database Scanner
 - 8. SQLPoke
 - 9. NGSSQLCrack

- 10. NGSSquirrel
- 11. SQLPing v2.2
- G. OLE DB Errors
- H. Input Validation Attack
- I. Login Guessing & Insertion
- J. Shutting Down SQL Server
- K. Extended Stored Procedures
- L. SQL Server Talks
- M. Preventive Measures

XV. Hacking Wireless Networks

- A. Introduction to Wireless Networking
- B. Business and Wireless Attacks
- C. Wireless Basics
- D. Components of Wireless Network
- E. Types of Wireless Network
- F. Setting up WLAN
- G. Detecting a Wireless Network
- H. How to access a WLAN
- I. Advantages and Disadvantages of Wireless Network
- J. Antennas
- K. SSIDs
- L. Access Point Positioning
- M. Rogue Access Points
- N. Tools to Generate Rogue Access Points
 - 1. Fake AP
 - 2. NetStumbler
 - 3. MiniStumbler
- O. What is Wireless Equivalent Privacy (WEP)?
- P. WEP Tool:
 - 1. AirSnort
 - 2. WEPCrack
- Q. Related Technology and Carrier Networks
- R. MAC Sniffing and AP Spoofing
- S. Tool to detect MAC Address Spoofing: Wellenreiter v2
- T. Terminology
- U. Denial of Service Attacks
- V. DoS Attack Tool: FATAjack
- W. Man-in-the-Middle Attack (MITM)
- X. Scanning Tools:
 - 1. Redfang
 - 2. Kismet
 - 3. THC- WarDrive v2.1
 - 4. PrismStumbler
 - 5. MacStumbler
 - 6. Mognet v1.16
 - 7. WaveStumbler
 - 8. StumbVerter v1.5

EC-Council Certified Network Defense Architect (CNDA)**Course Outline (con't)**

- 9. NetChaser v1.0 for Palm tops
 - 10. AP Scanner
 - 11. Wavemon
 - 12. Wireless Security Auditor (WSA)
 - 13. AirTraf 1.0
 - 14. Wifi Finder
 - Y. Sniffing Tools:
 - 1. AiroPeek
 - 2. NAI Sniffer Wireless
 - 3. Ethereal
 - 4. Aerosol v0.65
 - 5. vxSniffer
 - 6. EtherPEG
 - 7. Drifnet
 - 8. AirMagnet
 - 9. WinDump 3.8 Alpha
 - 10. ssidsniff
 - Z. Multi Use Tool: THC-RUT
 - AA. Tool: WinPcap
 - BB. Auditing Tool: bsd-airtools
 - CC. WIDZ- Wireless Detection Intrusion System
 - DD. Securing Wireless Networks
 - EE. Out of the box Security
 - FF. Radius: Used as Additional layer in security
 - GG. Maximum Security: Add VPN to Wireless LAN
- XVI. Virus and Worms**
- A. Virus Characteristics
 - B. Symptoms of 'virus-like' attack
 - C. What is a Virus Hoax?
 - D. Terminologies
 - E. How is a worm different from virus?
 - F. Indications of a Virus Attack
 - G. Virus History
 - H. Virus damage
 - I. Effect of Virus on Business
 - J. Access Methods of a Virus
 - K. Mode of Virus Infection
 - L. Life Cycle of a virus
 - M. What Virus Infect?
 - N. How virus infect?
 - O. Virus/worm found in the wild:
 - 1. W32.CIH.Spacefiller (a.k.a Chernobyl)
 - 2. Win32/Explore.Zip Virus
 - 3. I Love You Virus
 - 4. Melissa Virus
 - 5. Pretty Park
 - 6. Code red Worm
 - 7. W32/Klez
 - 8. Bug Bear
 - 9. SirCam Worm
 - 10. Nimda
 - 11. SQL Slammer
 - P. Writing a simple virus program
 - Q. Writing DDOS Zombie Virus
 - R. Virus Construction Kits
 - S. Virus Creation Scripts
 - T. Virus Detection Methods
 - U. Virus Incident Response
 - V. What is Sheep Dip?
 - W. Prevention is better than Cure
 - X. Anti-Virus Software
 - Y. Popular Anti-Virus packages
 - Z. New Virus found in 2004
 - AA. Virus Checkers
 - BB. Blaster – Virus Analysis
 - CC. Nimda – Virus Analysis
 - DD. Sasser Worm – Virus Analysis
 - EE. Klez – Virus Analysis
 - FF. IDAPro
 - GG. Virus Analyzers
- XVII. Physical Security**
- A. Security statistics
 - B. Physical Security breach incidents
 - C. Understanding Physical Security
 - D. What is the need of Physical Security?
 - E. Who is Accountable for Physical Security?
 - F. Factors affecting Physical Security
 - G. Physical Security checklist
 - 1. Company surroundings
 - 2. Premises
 - 3. Reception
 - 4. Server
 - 5. Workstation Area
 - 6. Wireless Access Points
 - 7. Other Equipments such as fax, removable media etc
 - 8. Access Control
 - 9. Computer Equipment Maintenance
 - 10. Wiretapping
 - 11. Remote access
 - H. Lock Picking Techniques
 - I. Spying Technologies
- XVIII. Linux Hacking**
- A. Why Linux?
 - B. Linux basics
 - C. Chrooting

EC-Council Certified Network Defense Architect (CNDA)**Course Outline (con't)**

- D. Why is Linux Hacked?
 - E. Linux Vulnerabilities in 2003
 - F. How to apply patches to vulnerable programs
 - G. Scanning Networks
 - H. Scanning Tool: Nessus
 - I. Cheops
 - J. Port Scan detection tools:
 - 1. Klaxon
 - 2. Scanlogd
 - 3. PortSentry
 - 4. LIDS (Linux Intrusion Detection System)
 - K. Password cracking in Linux
 - L. Password cracking tools:
 - 1. John the Ripper
 - 2. Viper
 - 3. Slurpie
 - M. IPChains
 - N. IPTables
 - O. ipchains vs. iptwadm
 - P. How to Organize Firewall Rules
 - Q. Security Auditor's Research Assistant (SARA)
 - R. Hacking Tool:
 - 1. Sniffit
 - 2. HPing2
 - 3. Hunt
 - 4. TCP Wrappers
 - S. Linux Loadable Kernel Modules
 - T. Linux Rootkits:
 - 1. Knark
 - 2. Torn
 - 3. Tuxit
 - 4. Adore
 - 5. Ramen
 - 6. Beast
 - U. Rootkit countermeasures:
 - 1. Chkrootki
 - 2. Tripwire
 - 3. Bastille Linux
 - 4. LIDS(Linux Intrusion Detection system)
 - 5. Dtk
 - 6. Rkdet
 - 7. Rootkit Hunter
 - 8. Carbonite
 - 9. Rscan
 - 10. Saint Jude
 - V. Linux Security Tools:
 - 1. Whisker
 - 2. Flawfinder
 - W. Advanced Intrusion Detection System (AIDE)
 - X. Linux Security testing tools
 - 1. NMap
 - 2. LSOF
 - 3. Netcat
 - 4. Nemesis
 - Y. Linux Encryption Tools:
 - 1. Stunnel
 - 2. OpenSSH/SSH
 - 3. SSH
 - 4. GnuPG
 - Z. Linux tools: Log and traffic monitors:
 - 1. MRTG
 - 2. Swatch
 - 3. Timbersee
 - 4. Logsurf
 - 5. IPLog
 - 6. IPTraf
 - 7. Ntop
 - AA. Linux Security Auditing Tool (LSAT)
 - BB. Linux Security countermeasures
- XIX. Evading Firewalls, IDS and Honeypots**
- A. Intrusion Detection Systems
 - B. Ways to Detect Intrusion
 - C. Types of Intrusion Detection System
 - D. Intrusion Detection Tools
 - 1. Snort 2.1.0
 - 2. Symantec ManHunt
 - 3. LogIDS 1.0
 - 4. SnoopNetCop Standard
 - 5. Prelude Hybrid IDS version 0.8.x
 - 6. Samhain
 - E. Steps to perform after an IDS detects an intrusion
 - F. Evading IDS systems
 - G. Tools to Evade IDS
 - 1. SideStep
 - 2. ADMutate
 - 3. Mendax v.0.7.1
 - 4. Stick
 - 5. Fragrouter
 - 6. Anzen NIDSbench
 - H. Packet Generators
 - I. Introduction to Firewalls
 - J. Firewall Identification
 - K. Firewalking
 - L. Banner Grabbing
 - M. Breaching Firewalls
 - N. Placing Backdoors through Firewalls
 - O. Hiding Behind Covert Channel: Loki

EC-Council Certified Network Defense Architect (CNDA)

Course Outline (con't)

- P. ACK tunneling
 - Q. Tools to Breach Firewall
 - 1. 007 Shell
 - 2. ICMP Shell
 - 3. AckCmd
 - 4. Covert TCP1.0
 - R. Tools for testing IDS and Firewalls
 - S. Introduction to Honeypots
 - T. Honeypot Project
 - U. Types of Honeypots
 - V. Honeypot: Specter
 - W. Honeypot: Honeyd
 - X. Honeypot: KFSensor
 - Y. Hacking Tool: Sebek
 - Z. Tools to Detect Honeypot
 - 1. Send-Safe Honeypot Hunter
 - 2. Nessus Security Scanner
- XX. Buffer Overflows**
- A. Significance of Buffer Overflow Vulnerability
 - B. Why are Programs/Applications Vulnerable?
 - C. Buffer Overflows
 - D. Reasons for Buffer Overflow Attacks
 - E. Knowledge required writing Buffer Overflow Exploits
 - F. How a Buffer Overflow occurs?
 - G. Understanding Stacks
 - H. Stack Implementation
 - I. Stack based buffer overflow
 - J. Shellcode
 - K. Heap Based buffer overflow
 - L. How to detect Buffer Overflows in a Program?
 - M. Attacking a real program
 - N. NOPS
 - O. How to mutate a Buffer Overflow Exploit? featuring ADMutate
 - P. Countermeasures
 - Q. Return Address Defender (RAD)
 - R. StackGuard
 - S. Immunix System
 - T. Vulnerability Search - ICAT
- XXI. Cryptography**
- A. Public-key Cryptography
 - B. Working of Encryption
 - C. Digital Signature
 - D. Digital Certificate
 - E. RSA (Rivest Shamir Adleman)
 - F. RSA Attacks
- 1. Brute forcing RSA factoring
 - 2. Esoteric attack
 - 3. Chosen cipher text attack
 - 4. Low encryption exponent attack
 - 5. Error analysis
 - 6. Other attacks
- G. MD5
 - H. SHA (Secure Hash Algorithm)
 - I. SSL (Secure Socket Layer)
 - J. RC5
 - K. What is SSH?
 - L. Government Access to Keys (GAK)
 - M. RSA Challenge
 - N. distributed.net
 - O. PGP (Pretty Good Privacy)
 - P. Code Breaking Methodologies
 - 1. Using Brute Force
 - 2. Frequency Analysis
 - 3. Trickery and Deceit
 - 4. One-Time Pad
 - Q. Cryptography Attacks
 - R. Disk Encryption
 - S. PGPCrack
 - T. Magic Lantern
 - U. WEPCrack
 - V. Cracking S/MIME Encryption using idle CPU Time
 - W. CypherCalc
 - X. Command Line Scriptor
 - Y. CryptoHeaven
- XXII. Penetration Testing**
- A. Need for a Methodology
 - 1. Penetration Test vs. Vulnerability Test
 - 2. Reliance on Checklists and Templates
 - 3. Phases of Penetration Testing
 - 4. Passive Reconnaissance
 - 5. Best Practices
 - 6. Results that can be expected
 - 7. Indicative passive reconnaissance steps include (but are not limited to)
 - 8. Introduction to Penetration Testing
 - 9. Type of Penetration Testing Methodologies
 - 10. Open Source Vs Proprietary Methodologies
 - 11. Security Assessment Vs Security Auditing
 - 12. Risk Analysis
 - 13. Types of Penetration Testing

EC-Council Certified Network Defense Architect (CNDA)**Course Outline (con't)**

14. Types Ethical Hacking
15. Vulnerability Assessment Vs Penetration Testing
16. Do-it Yourself Testing
17. Firms Offering Penetration Testing Services
18. Penetration Testing Insurance
19. Explication of Terms of Engagement
20. Pen-Test Service Level Agreements
21. Offer of Compensation
22. Starting Point and Ending Points of Testing
23. Penetration Testing Locations
24. Black Box Testing
25. White Box Testing
26. Grey Box Testing
27. Manual Penetration Testing
28. Automated Penetration Testing
29. Selecting the Right Tools
30. Pen Test Using Appscan
31. HackerShield
32. Pen-Test Using Cerberus Internet Scanner
33. Pen-Test Using CyberCop Scanner
34. Pen-Test Using Foundscan
35. Pen-Test Using Nessus
36. Pen-Test Using NetRecon
37. Pen-Test Using Retina
38. Pen-Test Using SAINT
39. Pen-Test Using SecureNET
40. Pen-Test Using SecureScan
41. Pen-Test Using SATAN, SARA and Security Analyzer
42. Pen-Test Using STAT Analyzer
43. Pen-Test Using Twscan
44. VigilEnt
45. WebInspect
46. Evaluating Different Types of Pen-Test Tools
47. Platform on Which Tools Will be Used
48. Asset Audit
49. Fault Tree and Attack Trees
50. GAP Analysis
51. Device Inventory
52. Perimeter Firewall Inventory
53. Web Server Inventory
54. Load Balancer Inventory
55. Local Area Network Inventory
56. Demilitarized Zone Firewall
57. Internal Switch Network Sniffer
58. Application Server Inventory
59. Database Server Inventory
60. Name Controller and Domain Name Server
61. Physical Security
62. ISP Routers
63. Legitimate Network Traffic Threat
64. Unauthorized Network Traffic Threat
65. Unauthorized Running Process Threat
66. Loss of Confidential Information
67. Business Impact of Threat
68. Pre-testing Dependencies
69. Post-testing Dependencies
70. Failure Management
71. Test Documentation Processes
72. Penetration Testing Tools
73. Defect Tracking Tools
74. Configuration Management Tools
75. Disk Replication Tools
76. Pen-Test Project Scheduling Tools
77. Network Auditing Tools
78. DNS Zone Transfer Testing Tools
79. Trace Route Tools and Services
80. Network Sniffing Tools
81. Denial of Service Emulation Tools
82. Traditional Load Testing Tools
83. System Software Assessment Tools
84. Operating System Protection Tools
85. Fingerprinting Tools
86. Port Scanning Tools
87. Directory and File Access Control Tools
88. File Share Scanning Tools
89. Password Directories
90. Password Guessing Tools
91. Link Checking Tools
92. Web site Crawlers
93. Web-Testing based Scripting Tools
94. Buffer Overflow Protection Tools
95. Buffer Overflow Generation Tools
96. Input Data Validation Tools
97. File encryption Tools
98. Database Assessment Tools
99. Keyboard Logging and Screen Reordering Tools
100. System Event Logging and Reviewing Tools
101. Tripwire and Checksum Tools

EC-Council Certified Network Defense Architect (CNDA)

Course Outline (con't)

- 102. Mobile-Code Scanning Tools
- 103. Centralized Security Monitoring Tools
- 104. Web Log Analysis Tools
- 105. Forensic Data and Collection Tools
- 106. Security Assessment Tools
- 107. Multiple OS Management Tools
- B. SANS Institute TOP 20 Security Vulnerabilities
 - 1. All Operating System Platforms
 - 2. Default installs of operating systems and applications
 - 3. Accounts with no passwords or weak passwords
 - 4. Nonexistent or incomplete backups
 - 5. Large number of open ports
 - 6. Not filtering packets for correct incoming and outgoing addresses
 - 7. Nonexistent or incomplete logging
 - 8. Vulnerable Common Gateway Interface (CGI) programs
 - 9. Windows-specific
 - 10. Unicode vulnerability-Web server folder traversal
 - 11. Internet server application programming interface (ISAPI) extension buffer overflows
 - 12. IIS Remote Data Services (RDS) exploit
 - 13. Network Basic Input Output System (NetBIOS), unprotected Windows networking shares
 - 14. Information leakage via null session connections
 - 15. Weak hashing in SAM (Security Accounts Manager)-LanManager hash
 - 16. UNIX-specific
 - 17. Buffer overflows in Remote Procedure Call (RPC) services
 - 18. Sendmail vulnerabilities
 - 19. Bind weaknesses
 - 20. Remote system command (such as rcp, rlogin, and rsh) vulnerabilities
 - 21. Line Printer Daemons (LPD) vulnerabilities
 - 22. Sadmin and mountd exploits
 - 23. Default Simple Network Management Protocol (SNMP) strings
- C. Penetration Testing Deliverable Templates
 - 1. Test Status Report Identifier
 - 2. Test Variances
 - 3. Test Comprehensive Assessment
 - 4. Summary of Results (Incidents)
 - 5. Test Evaluation
 - 6. Names of Persons (Approval)
 - 7. Template Test Incident Report
 - 8. Template Test Log
- D. Active Reconnaissance
- E. Attack Phase
- F. Activity: Perimeter Testing
- G. Activity: Web Application Testing – I
- H. Activity: Web Application Testing – II
- I. Activity: Wireless Testing
- J. Activity: Acquiring Target
- K. Activity: Escalating Privileges
- L. Activity: Execute, Implant & Retract
- M. Post Attack Phase & Activities
- N. Automated Penetration Testing Tool - CORE Impact