CURSO DE HACKING ETICO

En este curso el participante comprenderá la metodología del etical hacking y penetration testing.

Dirigido :

Este curso esta dirigido a administradores de red, administradores de seguridad, y a todas las personas que estén interesadas en el etical hacking y penetration testing.

Requerimientos:

Conocimientos de TCP/IP, Windows, Linux (básico)

Material del curso:

- 1 Carpeta
- CD con herramientas
- CD con información adicional
- Material impreso con el desarrollo del curso

Nota: Los Módulos 19, 20, 21, 22 son tentativos

Contenido del curso :

Module 1: Introduction to Ethical Hacking

• 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 Law).

Module 2: Footprinting

• Defining Footprinting.
• Information Gathering Methodology.
• Locate the Network Range.
• Hacking Tools:
o Whois
o Nslookup
o ARIN
o Traceroute

- NeoTrace
- VisualRoute Trace
- SmartWhois
- Visual Lookout
- VisualRoute Mail Tracker
- eMailTrackerPro
- e-mail Spider
- Wayback machine

Module 3: Scanning

• Definition of Scanning.
• Types of scanning
• Objectives of Scanning
• Scanning Methodology
• Classification of Scanning
• Hacking Tools
- Nmap
- 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

Module 4: Enumeration

• What is Enumeration?
• NetBios Null Sessions
• Hacking Tools
o DumpSec
o Winfo
o NetBIOS Auditing Tool (NAT)
• Null Session Countermeasures
• NetBIOS Enumeration
• Hacking Tool :NBTScan
• Simple Network Management Protocol (SNMP)
Enumeration
• Hacking Tools
o Solarwinds
o Enum
o SNScan
• SNMP Enumeration Countermeasures
• Management Information Base (MIB)
• Windows 2000 DNS Zone Transfer
• Blocking Win 2k DNS Zone Transfer
• Enumerating User Accounts
• Hacking Tools
o User2sid and Sid2user
o UserInfo
o GetAcct
o DumpReg
o Trout
o Winfingerprint
o PsTools
(PSFile,PSLoggedOn,PSGetSid,PSInfo,PSService,P
SList,PSKill, PSSuspend, PSLogList, PSExec, PSShutdown)
• Active Directory Enumeration and Countermeasures

Module 5: System Hacking

• Administrator Password Guessing
• Manual Password Cracking Algorithm
• Automated Password Cracking
• Password Types
• Types of Password Attacks
• Hacking Tool
o NTInfoScan (CIS)
• Performing Automated Password Guessing
• Hacking Tool
• Legion
• Password Sniffing
• Hacking Tools
o LOphtcrack
o pwdump2 and pwdump3
o KerbCrack
o 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

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

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

• Countermeasures

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
- Trino0

- 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

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 ExploitTool
  - 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

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

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
o LOphtcrack
o John The Ripper
o Brutus
o Obiwan
o Authforce
o Hydra
o Cain and Abel
o RAR
o Gammaprog
• Hacking Tools:
o WebCracker
o Munga Bunga
o PassList
o Read Cookies
o SnadBoy
o 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
o SQLDict
o SqlExec
o SQLbf
o SQLSmack
o SQL2.exe

o 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

Module 15: Hacking Wireless Networks

• Introduction to Wireless Networking
• Business and Wireless Attacks
• 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

Module 16 : Virus

• 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

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
o Company surroundings
o Premises
o Reception
o Server
o Workstation Area
o Wireless Access Points
o Other Equipments such as fax, removable media etc
o Access Control
o Computer Equipment Maintenance
o Wiretapping
o 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:

o Klaxon
o 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

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

Module 21 : Cryptography

• Public-key Cryptography
• Working of Encryption
• Digital Signature
• Digital Certificate
• RSA (Rivest Shamir Adleman)
• RSA Attacks
o Brute forcing RSA factoring
o Esoteric attack
o Chosen cipher text attack
o Low encryption exponent attack
o Error analysis
o 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
o Using Brute Force
o Frequency Analysis

o Trickery and Deceit
o 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
• Tool: CORE Impact

Duración: 36 hrs.