CETPA INFOTECH PVT. LTD.

Curriculum of CYBER SECURITY

DURATION: 6 MONTHS

Implementing Cisco IOS Network Security

1.0 Common Security Threats

1.1 Describe common security threats

- 1.1.a Common threats to the physical installation
- 1.1.b Mitigation methods for common network attacks
- 1.1.c Email-based threats
- 1.1.d Web-based attacks
- 1.1.e Mitigation methods for Worm, Virus, and Trojan Horse attacks
- 1.1.f Phases of a secure network lifecycle
- 1.1.g Security needs of a typical enterprise with a comprehensive security policy
- 1.1.h Mobile/remote security
- 1.1.i DLP

2.0 Security and Cisco Routers

2.1 Implement security on Cisco routers

- 2.1.a CCP Security Audit feature
- 2.1.b CCP One-Step Lockdown feature
- 2.1.c Secure router access using strong encrypted passwords, and using IOS login enhancements, IPV6 security.
- 2.1.d Multiple privilege levels
- 2.1.e Role-based CLI
- 2.1.f Cisco IOS image and configuration files

2.2 Describe securing the control, data and management plane

2.3 Describe CSM

2.4 Describe IPv4 to IPv6 transition

- 2.4.a Reasons for IPv6
- 2.4.b Understanding IPv6 addressing
- 2.4.c Assigning IPv6 addresses
- 2.4.d Routing considerations for IPv6

3.0 AAA on Cisco Devices

3.1 Implement authentication, authorization, and accounting (AAA)

3.2 Describe TACACS+

3.3 Describe RADIUS

3.4 Describe AAA

- 3.4.a Authentication
- 3.4.b Authorization
- 3.4.c Accounting

3.5 Verify AAA functionality.

4.0 IOS ACLs

4.1 Describe standard, extended, and named IP IOS ACLs to filter packets

- 4.1.a IPv4
- 4.1.b IPv6
- 4.1.c Object groups
- 4.1.d ACL operations
- 4.1.e Types of ACLs (dynamic, reflexive, time-based ACLs)
- 4.1.f ACL wild card masking
- 4.1.g Standard ACLs
- 4.1.h Extended ACLs
- 4.1.i Named ACLs
- 4.1.j VLSM

4.2 Describe considerations when building ACLs

- 4.2.a Sequencing of ACEs
- 4.2.b Modification of ACEs

4.3 Implement IP ACLs to mitigate threats in a network

- 4.3.a Filter IP traffic
- 4.3.b SNMP
- 4.3.c DDoS attacks
- 4.3.d CLI
- 4.3.e CCP
- 4.3.f IP ACLs to prevent IP spoofing
- 4.3.g VACLs

5.0 Secure Network Management and Reporting

5.1 Describe secure network management

- 5.1.a In-band
- 5.1.b Out of band
- 5.1.c Management protocols
- 5.1.d Management enclave
- 5.1.e Management plane

5.2 Implement secure network management

- 5.2.a SSH
- 5.2.b syslog
- 5.2.c SNMP
- 5.2.d NTP
- 5.2.e SCP
- 5.2.f CLI
- 5.2.g CCP
- 5.2.h SSL

6.0 Common Layer 2 Attacks

6.1 Describe Layer 2 security using Cisco switches

- 6.1.a STP attacks
- 6.1.b ARP spoofing
- 6.1.c MAC spoofing
- 6.1.d CAM overflows
- 6.1.e CDP/LLDP

6.2 Describe VLAN Security

- 6.2.a Voice VLAN
- 6.2.b PVLAN
- 6.2.c VLAN hopping
- 6.2.d Native VLAN

6.3 Implement VLANs and trunking

- 6.3.a VLAN definition
- 6.3.b Grouping functions into VLANs
- 6.3.c Considering traffic source to destination paths
- 6.3.d Trunking
- 6.3.e Native VLAN
- 6.3.f VLAN trunking protocols
- 6.3.g Inter-VLAN routing

6.4 Implement Spanning Tree

- 6.4.a Potential issues with redundant switch topologies
- 6.4.b STP operations
- 6.4.c Resolving issues with STP

7.0 Cisco Firewall Technologies

7.1 Describe operational strengths and weaknesses of the different firewall technologies

- 7.1.a Proxy firewalls
- 7.1.b Packet and stateful packet
- 7.1.c Application firewall
- 7.1.d Personal firewall

7.2 Describe stateful firewalls

- 7.2.a Operations
- 7.2.b Function of the state table

- 7.3 Describe the types of NAT used in firewall technologies
  - 7.3.a Static
  - 7.3.b Dynamic
  - 7.3.c PAT

- 7.4 Implement Zone Based Firewall using CCP
  - 7.4.a Zone to zone
  - 7.4.b Self zone

- 7.5 Implement the Cisco Adaptive Security Appliance (ASA)
  - 7.5.a NAT
  - 7.5.b ACL
  - 7.5.c Default MPF
  - 7.5.d Cisco ASA sec level

- 7.6 Implement NAT and PAT
  - 7.6.a Functions of NAT, PAT, and NAT Overload
  - 7.6.b Translating inside source addresses
  - 7.6.c Overloading Inside global addresses

8.0 Cisco IPS

- 8.1 Describe IPS deployment considerations
  - 8.1.a SPAN
  - 8.1.b IPS product portfolio
  - 8.1.c Placement
  - 8.1.d Caveats
  - 8.2 Describe IPS technologies
  - 8.2.a Attack responses
  - 8.2.b Monitoring options
  - 8.2.c syslog
  - 8.2.d SDEE
  - 8.2.e Signature engines
  - 8.2.f Signatures
  - 8.2.g Global correlation and SIO
  - 8.2.h Network-based
  - 8.2.i Host-based

- 8.3 Configure Cisco IOS IPS using CCP
  - 8.3.a Logging
  - 8.3.b Signatures

9.0 VPN Technologies

- 9.1 Describe the different methods used in cryptography
  - 9.1.a Symmetric
  - 9.1.b Asymetric
  - 9.1.c HMAC
  - 9.1.d Message digest
  - 9.1.e PKI

- 9.2 Describe VPN technologies
  - 9.2.a IPsec
  - 9.2.b SSL

- 9.3 Describe the building blocks of IPSec
  - 9.3.a IKE
  - 9.3.b ESP
  - 9.3.c AH
  - 9.3.d Tunnel mode
  - 9.3.e Transport mode

- 9.4 Implement an IOS IPSec site-to-site VPN with pre-shared key authentication
  - 9.4.a CCP
  - 9.4.b CLI
  - 9.5 Verify VPN operations.

- 9.6 Implement SSL VPN using ASA device manager
  - 9.6.a Clientless
  - 9.6.b Any Connect

1. Introduction to Ethical Hacking

- Information Security Overview
- Information Security Threats and Attack Vectors
- Top Information Security Attack Vectors
- Motives, Goals, and Objectives of Information Security Attacks
- Information Security Threats
- Information Warfare
- IPv6 Security Threats
- Hacking Concepts
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who Is a Hacker?
- Hacker Classes
- Hacktivism
- Hacking Phases
- Types of Attacks
- Types of Attacks on a System
- Operating System Attacks
- Misconfiguration Attacks
- Application-Level Attacks
- Skills of an Ethical Hacker
- Defense in Depth
- Incident Management Process
- Information Security Policies
- Classification of Security Policies
- Structure and Contents of Security Policies

2. Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting Terminology
- What is Footprinting?
- Why Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Footprinting through Search Engines
- Finding Company's External and Internal URLs
- Mirroring Entire Website
- Website Mirroring Tools
- Extract Website Information from http://www.archive.org
- Monitoring Web Updates Using Website Watcher
- Finding Resources Using Google Advance Operator
- Google Hacking Tool: Google Hacking Database (GHDB)
- Google Hacking Tools
- WHOIS Footprinting
- WHOIS Lookup
- DNS Footprinting
- Extracting DNS Information
- DNS Interrogation Tools
- Network Footprinting
- Locate the Network Range
- Determine the Operating System
- Footprinting through Social Engineering

3. Scanning Networks

- Check for Live Systems
- Checking for Live Systems - ICMP Scanning
- Ping Sweep
- Check for Open Ports
- Scanning Tool: Nmap
- Hping2 / Hping3
- Scanning Techniques
- Scanning Tool: NetScan Tools Pro
- Scanning Tools
- Do Not Scan These IP Addresses (Unless you want to get into trouble)
- Port Scanning Countermeasures
- Banner Grabbing Countermeasures: Disabling or Changing Banner
- Hiding File Extensions from Web Pages
- Scan for Vulnerability
- Proxy Servers
- Why Attackers Use Proxy Servers?
- Use of Proxies for Attack

4. Enumeration

- What is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate
- NetBIOS Enumeration
- NetBIOS Enumeration
- NetBIOS Enumeration Tool: SuperScan
- NetBIOS Enumeration Tool: Hyena
- NetBIOS Enumeration Tool: Winfingerprint
- NetBIOS Enumeration Tool: NetBIOS Enumerator
- Enumerating User Accounts

5. System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- CEH System Hacking Steps
- CrackingPasswords
- Password Cracking
- Password Complexity
- Password Cracking Techniques
- Types of Password Attacks
- Distributed Network Attack
- Default Passwords
- Manual Password Cracking (Guessing)
- Stealing Passwords Using Keyloggers
- Spyware
- How to Defend Against Keyloggers
- Anti-Spywares
- What Is Steganography?
- Least Significant Bit Insertion

6. Trojans and Backdoors

- Trojan Concepts
- What is a Trojan?
- Trojan Infection
- Types of Trojans
- Command Shell Trojans
- Command Shell Trojan: Netcat
- GUI Trojan: MoSucker
- GUI Trojan: Jumper and Biodox
- Document Trojans
- E-mail Trojans
- E-mail Trojans: RemoteByMail
- Trojan Detection
- How to Detect Trojans
- Scanning for Suspicious Ports
- Trojan Horse Construction Kit
- Anti-Trojan Software

7. Viruses and Worms

- Virus and Worms Concepts
- Introduction to Viruses
- Virus and Worm Statistics
- Types of Viruses
- System or Boot Sector Viruses
- File and Multipartite Viruses
- Macro Viruses
- Cluster Viruses
- Stealth/Tunneling Viruses
- Encryption Viruses
- Polymorphic Code
- Computer Worms
- Malware Analysis
- Online Malware Testing: VirusTotal
- Online Malware Analysis Services
- Anti-virus Tools

8. Sniffers

- Sniffing Concepts
- Wiretapping
- Lawful Interception
- Packet Sniffing
- Sniffing Threats
- SPAN Port
- MAC Attacks
- MAC Flooding
- MAC Address/CAM Table
- How CAM Works
- DHCP Attacks
- How DHCP Works
- DHCP Request/Reply Messages
- IPv4 DHCP Packet Format
- ARP   Poisoning
- What Is Address Resolution Protocol (ARP)?
- ARP Spoofing Techniques
- ARP Spoofing Attack
- Spoofing Attack
- Spoofing Attack Threats
- DNS Poisoning
- DNS Poisoning Techniques

9. Social Engineering

- Social Engineering Concepts
- What is Social Engineering?
- Behaviors Vulnerable to Attacks
- Social Engineering Techniques
- Types of Social Engineering
- Human-based Social Engineering
- Technical Support Example
- Authority Support Example
- Social Networking Sites
- Social Engineering Through Impersonation on Social Networking Sites
- How to Detect Phishing Emails
- Anti-Phishing Toolbar: Netcraft
- Anti-Phishing Toolbar: PhishTank
- Identity Theft Countermeasures

10. Denial of Service

- DoS/DDoS Concepts
- What is a Denial of Service Attack?
- What Are Distributed Denial of Service Attacks?
- Symptoms of a DoS Attack
- DoS Attack Techniques
- Bandwidth Attacks
- Service Request Floods
- SYN Attack
- SYN Flooding
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Permanent Denial-of-Service Attack
- Application Level Flood Attacks
- Botnet
- Botnet Propagation Technique
- DDoS Attack
- DDoS Attack Tool: LOIC
- DoS Attack Tools

11. Session Hijacking

- Session Hijacking Concepts
- What is Session Hijacking?
- Dangers Posed by Hijacking
- Why Session Hijacking is Successful?
- Key Session Hijacking Techniques
- Brute Forcing Attack
- Network-level Session Hijacking
- The 3-Way Handshake
- Sequence Numbers
- Session Hijacking Tools
- Session Hijacking Tool: Zaproxy
- Session Hijacking Tool: Burp Suite
- Session Hijacking Tool: JHijack
- Session Hijacking Tools

12. Hacking Webservers

- Webserver Concepts
- Webserver Market Shares
- Open Source Webserver Architecture
- Attack Methodology
- Webserver Attack Methodology
- Webserver Attack Methodology: Information Gathering
- Webserver Attack Methodology: Webserver Footprinting
- Counter-measures
- Countermeasures: Patches and Updates
- Countermeasures: Protocols
- Countermeasures: Accounts
- Countermeasures: Files and Directories
- How to Defend Against Web Server Attacks
- How to Defend against HTTP Response Splitting and Web Cache Poisoning
- Web Server Penetration Testing

13. Hacking Web Applications

- Web App Concepts
- Web Application Security Statistics
- Introduction to Web Applications
- SQL Injection Attacks
- Command Injection Attacks
- Web App Hacking Methodology
- Footprint Web Infrastructure
- Footprint Web Infrastructure: Server Discovery
- Hacking Web Servers
- Web Server Hacking Tool: WebInspect
- Web Services Probing Attacks
- Web Service Attacks: SOAP Injection
- Web Service Attacks: XML Injection
- Web Services Parsing Attacks
- Web Service Attack Tool: soapUI

14. SQL Injection

- SQL Injection Concepts
- SQL Injection
- Scenario
- SQL Injection Threats
- What is SQL Injection?
- SQL Injection Attacks
- SQL Injection Detection
- Types of SQL Injection
- Simple SQL Injection Attack
- Union SQL Injection Example
- SQL Injection Error Based
- Blind SQL Injection
- What is Blind SQL Injection?
- SQL Injection Methodology
- Advanced SQL Injection
- Information Gathering
- Extracting Information through Error Messages
- Interacting with the FileSystem
- SQL Injection Tools
- SQL Injection Tools: BSQLHacker
- SQL Injection Tools: Marathon Tool
- SQL Injection Tools: SQL Power Injector
- SQL Injection Tools: Havij
- SQL Injection Tools

15. Hacking Wireless Networks

- Wireless Concepts
- Wireless Networks
- Wi-Fi Networks at Home and Public Places
- Types of Wireless Networks
- Wireless Encryption
- Wireless Threats
- Wireless Threats: Access Control Attacks
- Wireless Threats: Integrity Attacks
- Footprint the Wireless Network
- Attackers Scanning for Wi-Fi Networks
- Bluetooth Hacking
- Bluetooth Threats

16. Evading IDS, Firewalls, and Honeypots

- IDS, Firewall and Honeypot Concepts
- How IDS Works?
- Ways to Detect an Intrusion
- Denial-of-Service Attack (DoS)
- ASCII Shellcode
- Other Types of Evasion
- Evading Firewalls
- IP Address Spoofing
- Source Routing
- Website Surfing Sites
- Detecting Honeypots
- Detecting Honeypots

17. Buffer Overflow

- Buffer Overflow Concepts
- Buffer Overflow
- Shellcode
- No Operations (NOPs)
- Buffer Overflow Methodology
- Overflow using Format String
- Smashing the Stack
- Once the Stack is Smashed...
- Buffer Overflow Security Tools
- BoF Security Tool: BufferShield
- BoF Security Tools

18. Cryptography

- Cryptography Concepts
- Cryptography
- Types of Cryptography
- Government Access to Keys (GAK)
- Encryption Algorithms
- Ciphers
- Advanced Encryption Standard (AES)
- Public Key Infrastructure(PKI)
- Public Key Infrastructure (PKI)
- Certification Authorities
- Email Encryption
- Digital Signature
- SSL (Secure Sockets Layer)
- Transport Layer Security (TLS)
- Disk Encryption Tools
- Cryptanalysis Tool: CrypTool
- Cryptanalysis Tools
- Online MD5 Decryption Tool

19. Penetration Testing

- Pen Testing Concepts
- Security Assessments
- Security Audit
- Vulnerability Assessment
- Limitations of Vulnerability Assessment
- Introduction to Penetration Testing
- Penetration Testing
- Why Penetration Testing?
- Testing Locations
- Types of Pen Testing
- Types of Penetration Testing
- External Penetration Testing
- Internal Security Assessment
- Black-box Penetration Testing
- Grey-box Penetration Testing
- White-box Penetration Testing

Head Office: 200 Purwavali, 2nd Floor, (Opp. Railway Ticket Agency), Railway Road, Ganeshpur,
Roorkee-247667
Ph. No.:+91-9219602769, +91-1332-270218 Fax No. :+91-1332-274960

Corporate Office: D-58, Sector-2, In Red FM. Noida Lane, Noida-201301
Ph. No.:+91-9212172602, +91-120-4535353

Branch Office: 401 A, 4th Floor, LekhrajKhazana, Faizabad Road, Indira Nagar, Lucknow-226016
Ph. No. +91-522-6590802, +91-9258017974, Fax No.: +91-522-6590802

Branch Office: 105, MohitVihar, Near Kamla Palace, GMS Road, Dehradun-248001
Ph. No.: +91-9219602771, +91-0135-6006070

CETPA®
Because Knowledge Matters
ISO 9001 : 2008 Certified

Toll Free- 1800-8333-999(From Any Network)