

# Course Curriculum



## CCNA

### Introduction to Networking

- Introduction to Networking
- Network Topologies
- Networking Devices

### OSI Reference model

- The OSI Reference Model Overview
- The TCP/IP Stack
- Data encapsulation

### Working with Ethernet

- Fundamentals of Ethernet
- Ethernet Frame Format
- Hub vs Switch
- ARP and MAC address table
- Cabling Types (Co-axial, Twisted Pair, Optical Fibre)
- Cable Issues (collisions, errors, duplex, speed)
- Connectors
- PoE Concept

# Introduction to Cisco IOS

- Navigating the Cisco IOS Operating System
- Cisco IOS Configuration Management
- Cisco Networking LAB

# Understanding TCP & UDP

- Transport Layer Header Format
- TCP and UDP
- Port Numbers
- The Network Layer
- The IP Header Format
- Unicast, Multicast and Broadcast Traffic

# Introduction to IP addressing & subnetting

- Number System
- Binary representation of IP
- IPv4 Addresses Classes
- IPv4 Subnetting
- VLSM Calculation



# Working with layer 2 Switches

- Switch Configuration
- Speed and Duplex Settings
- CDP and LLDP
- Port security
- Basic Layer 1 and 2 Troubleshooting

# Managing Cisco Devices

- Cisco Device Management
- The Boot Up Process
- Factory Reset and Password Recovery
- Backing up the System Image and Configuration
- Upgrading IOS

## **Understanding & configuring routing protocols**

- Routing Fundamentals Dynamic Routing
- Protocols vs Static Routes Static Routes
- Default Routes Summarisation Longest Prefix
- Match Routing Protocol Types Routing
- Protocol Metrics Equal Cost Multi Path
- Administrative Distance Loopback Interfaces
- RIP Routing
- 
- 
- 
- 
- 

### **EIGRP Routing**

- EIGRP operations DUAL Algorithm features
- Configuring & implementing EIGRP (IPv4)
- Configuring & implementing EIGRP (IPv6)
- EIGRP Authentication Configuring Load balancing in EIGRP
-

# **OSPF Routing**

- Introducing link state routing protocol
- OSPF protocol and Operations
- OSPF terminology and Packet Type
- Discussing OSPF Protocol States
- DR and BDR Election process
- Configuring OSPF with single area. Configure and verify OSPF
- Neighbour adjacencies
- OSPF states
- Router LSA types

## **Configuring DHCP on Cisco Devices**

- DHCP Dynamic Configuration Protocol
- Cisco DHCP Server
- DHCP relay
- Windows, Mac and Linux client IP settings
- Cisco DHCP Client
- DHCP snooping
- Connectivity Troubleshooting
- Cisco Troubleshooting Methodology

## **Working with VLAN**

- Campus LAN Design - Core, Distribution and Access Layers
- Spine-Leaf Network Design
- 802.1Q and Native VLAN
- VLAN Access and Trunk Ports
- DTP Dynamic Trunking Protocol
- VTP VLAN Trunking Protocol
- Inter-VLAN Routing

# **First Hop Redundancy Protocols**

- Network Redundancy
- FHRP First Hop Redundancy Protocols
- HSRP Hot Standby Router Protocol
- HSRP Advanced Topics

# **Spanning Tree Protocols**

- Spanning Tree Protocol
- Spanning Tree working and port states
- Rapid PVST+
- Manipulating the Root Bridge Election
- Spanning Tree and HSRP Alignment
- PortFast, BPDU Guard and Root Guard
- STP Troubleshooting

# **Network bonding**

- EtherChannel (LACP, PAgP)
- EtherChannel Load Balancing
- EtherChannel Protocols and Configuration
- Layer 3 EtherChannel

# **Protocol overview**

- Overview of Protocols
- DHCP, DNS, HTTP, Telnet, SSH, NTP, HTTPS, SNMP, ICMP, POP3, IMAP, SMTP, TFTP, FTP

# **Configuring ACL**

- ACL Overview
- Configuring Standard, Extended and Named ACLs

# **Network Address Translation**

- IPv4 Address Exhaustion and NAT
- Static NAT
- Dynamic NAT
- PAT Port Address Translation

## **Introduction to IPv6**

- The IPv6 Address Format
- IPv6 Global Unicast Addresses
- EUI-64 Addresses
- Unique Local and Link Local Addresses
- Anycast and Multicast
- SLAAC Stateless Address Autoconfiguration
- IPv6 Static Routes

## **Wide Area Networks**

- WAN Overview
- VPN - Virtual Private Networks
- Metro Ethernet
- MPLS Multi-Protocol Label Switching
- PPPoE Point to Point Protocol over Ethernet
- WAN Topology Options

## **Security Fundamentals**

- The Security Threat Landscape
- Common Attacks
- Firewalls and IDS/IPS
- Firewalls vs Packet Filters

- Cryptography
- TLS Transport Layer Security
- Site-to-Site VPN Virtual Private Networks
- Remote Access VPN Virtual Private Networks
- Threat Defence Solutions
- Line Level Security
- Privileged Exec and Password Encryption
- Usernames and Privilege Levels
- SSH Secure Shell
- AAA Authentication, Authorization and Accounting
- Global Security Best Practices

## Monitoring & Traffic Shaping

- Syslog Terminal Monitor and Logging
- Synchronous SNMP Simple Network Management Protocol QoS Overview
- Classification and Marking Congestion
- Management Policing and Shaping
- 
- 

## IT Services

- Traditional IT Deployment Models
- Defining Cloud Computing
- Cloud Computing Case Study
- Server Virtualization
- Virtualizing Network Devices
- Cloud Service Models
- Cloud Deployment Models
- Cloud Computing Advantages

# Wireless Networks

- Wireless Network Types Infrastructure Mode and
- Wireless Access Points Wireless LAN Controllers
- and CAPWAP Switch Configuration for Wireless
- Networks Wireless Channels and Radio
- Frequencies Wireless Security (WPA, WPA2 and
- WPA3)

# Network Automation

- The Benefits of Network Automation and Programmability
- Python, Git, GitHub and CI-CD
- Data Serialization Formats: XML, JSON and YAML
- APIs - CRUD, REST and SOAP
- Configuration Management Tools - Ansible, Puppet and Chef
- SDN Software Defined Networking
- Ansible LAB



# Cybersecurity

- Introduction to Cybersecurity
- Challenges of protecting electronic information
- Using the Lab simulator

## Access Control and Identity management

- Introduction to Identity management Controlling access to system resources Access control models, terminology, best practices, tools Remote and network considerations to controlling access.

## Cryptography

Introduction to cryptography

Cryptographic attacks and the tools to ensure data integrity

Hashing, symmetric and asymmetric encryption, and certificates

Methods of implementing cryptography

## Policies, Procedures, and Awareness

- Security policies, procedures and security awareness
- Security classification levels, documents
- Business continuity plans, risk management considerations, incident response
- Trusted computing, software development concerns, and management of employees.

## Physical Security

- Fundamentals of physically securing access to facilities and computer systems
- Protecting a computer system with proper environmental conditions and fire-suppression systems
- Securing mobile devices and telephony transmissions.

# **Perimeter** Defences

- Perimeter defences to increase network security
- Perimeter attacks, security zones and devices
- Configuring a DMZ, firewalls, NAT router, VPNs, protections against web threats
- Network Access Protection (NAP) and security for wireless networks.

# **Network** Defences

- Introduction to Network Defences
- Network device vulnerabilities and defences
- Providing security for a router and switch
- Implementing intrusion monitoring and prevention.

# **Host** defences

- Introduction Host Defences
- Types of malware and how to protect against them
- Protecting against password attacks recommendations for hardening a Windows system
- Configuring GPOs to enforce security, managing file system security
- Procedures to increase network security of a Linux system.

# **Application** defences

- Introduction to Application Defences
- Basic concepts of securing web applications from attacks
- Fortifying the internet browser, securing e-mail from e-mail attacks
- Concerns about networking software,& security considerations when using a virtual machine.

# **Data** defences

- Introduction to Data Defences
- Elements of securing data, such as, implementing redundancy through RAID
- Proper management of backups and restores, file encryption
- Implementing secure protocols, and cloud computing.

# Ethical Hacking

- Hacking concept, what is hacking?
- Terms we use in hacking.
- Need of Ethical hacking.
- Cases of Hacking in India & across the globe
- Types of Hacking
- Building the foundation for Ethical hacking
- Hacking Phases
- Types of Hackers
- Roles and Responsibilities
- Advantages & scope for hacking
- Drawbacks & Limitation of hacking
- Threats & categories
- Attack Vectors and Exploitation
- Common Hacking Tools
- Hacking Techniques & Approaches

## Policies and Controls

- Risk Management & Incident Management
- Information Security controls
- Data Management
- Concept of Penetration testing
- Types of Penetration testing
- Phases of Penetration testing
- Vulnerability Assessment by Penetration testing

# **Viruses, Trojans, Malwares, & OS Level Attacks & Counter Measures**

- Introduction to Malware
- Different Ways a Malware can Get into a System
- Common Techniques Attackers Use to Distribute Malware on the Web
- Components of Malware
- Introduction to Viruses, Worms & Trojan
- Types of Virus, Worms & Trojan
- Fake Antiviruses
- How Did Antivirus Works
- Introduction to Malware Analysis
- Malware Analysis Procedure
- Malware Detection Method

## **Foot printing, Enumeration, Scanning, Sniffing, Social Engineering**

- Information Gathering Using Google Advanced Search and Image Search
- VoIP and VPN Footprinting through Google Hacking Database
- Finding Company's Top-level Domains (TLDs) and Sub-domains
- Finding Location, People search, Professional search
- Techniques for Enumeration, Services and Ports to Enumerate
- NetBIOS, SNMP, LDAP Enumeration
- Information Gathering Using Groups, Forums, and Blogs
- Network Scanning Concepts
- Scanning Tools and Techniques
- Scanning Pen Testing
- Port Scanning & Countermeasures
- Sniffing Concepts & Techniques
- Wireshark installing & concept
- Sniffing Detection Techniques
- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threat / Insider Attack

Social Engineering Countermeasures

📞: 8919210748/8897814073

✉️: codingcreatros@gmail.com

# **SQL Injection, DOS Attacks, Session hijacking and System hacking**

- Basics to the SQL queries How
- Injection Can be done Cross Site
- ScrlPting Attacks DoS/DDoS
- Attack Techniques DDoS Case
- Study DoS/DDoS Attack Tools
- Session Hijacking Concepts
- Network Level Session Hijacking
- System Hacking Concepts
- Cracking Passwords Escalating
- Privileges Hiding Files and
- Covering tracks Client side
- Hijacking
- 
- 

## **Web Applications, Servers attacking & Counter measures**

- Basics of Web Application and Technology stack.
- OWASP Top 10 Application Security Risks - 2017
- Injection Flaws File Injection Attack Broken
- Authentication Sensitive Data Exposure XML External
- Entity (XXE) Broken Access Control Security
- Misconfiguration Cross-Site ScrlPting (XSS) Attacks
- Insecure Deserialization Using Components with Known Vulnerabilities Web App Hacking Methodology
- and its foot printing
- 
- 
-

- Password Attacks
- Password Functionality Exploits
- Password Guessing and Brute-forcing
- Web Server Concepts
- Web server attacks
- Web Server Attack Methodology
- Web Server Attack Tools
- Detecting Web Server Hacking Attempts
- Patch Management
- Web Server Security Tools

## **IoT and Cloud Attacks and Defense Mechanisms**

- Basic of IOT, Architecture, Technology and Protocols
- Challenges, Opportunity in IOT
- OWASP Top 10 IOT Vulnerabilities and Obstacles
- DDos Attack
- Jamming Attack
- Botnets
- Man In middle concept
- Data & Identity Theft
- Introduction to Cloud & Virtualization
- Cloud Deployment and responsibilities
- Service Hijacking
- Social Engineering
- Network sniff
- XSS attack
- DNS (Domain Name system attack)
- Control Layers and Responsibilities
- Cloud Computing Security Consideration
- 
-

# **Mobile & Wireless Networks Hacking and Counter measures**

- Introduction to the Mobile architecture
- Working principle for mobile OS
- Security of the application used in Mobiles
- Hacking Methodology for mobile with Metasploit
- Introduction to Terminology, Networks, Standards
- Types of Wireless Authentication and Encryption
- WEP (Wired Equivalent Privacy) Encryption
- WPA (Wi-Fi Protected Access) Encryption
- WPA2 (Wi-Fi Protected Access 2) Encryption
- Wi-Fi Discovery
- GPS Mapping
- Traffic canalizing
- Launch Wireless attacks
- Crack Wi-Fi Encryption

## **Firewall, IDS & honeypot evasion techniques, tools, & countermeasures**

- What is Firewall & Example
- What is IDS & example
- What is Honeypots & examples
- Case study of Bypassing Firewall ,IDS, Firewall  
What is Firewall & Examples
- What is IDS & example
- What is Honeypots & examples
- Case study of Bypassing Firewall ,IDS, Firewall
- Packet Fragmentation and Source Routing
- Working with SNORT [Detection Tool]
- IP address Decoy and Spoofing
-

- IP Spoofing Detection Techniques: Direct TTL Probes
- IP Spoofing Detection Techniques: IP Identification Number
- IP Spoofing Detection Techniques: TCP Flow Control Method
- IP Spoofing Countermeasures

## **Cryptology, Vulnerability Analysis, Logging and Audit**

- Types of Cryptography
- Government Access to Keys (GAK)
- CIPhers
- Data Encryption Standard
- Advanced Encryption Standard
- RC4, RC5, and RC6 Algorithms
- Digital Signature, SSL, TLS
- Cryptography Toolkit & Disk Encryption
- Brute-Force Attack
- Meet-in-the-Middle Attack on Digital Signature Scheme
- Side Channel Attack
- Hash Collision Attack
- DUHK Attack
- Rainbow Table Attack
- Vulnerability Assessment Concept & Solutions
- Vulnerability Assessment Tools & Reports
- Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

# Capture the flag [CTF]

- Understanding of Kali Linux commands
- Using commands situation based
- Understanding of web application
- Web application tricks to get data
- Doing pentesting Situation based
- Installing and working on Kali Linux
- Vulnerability Assessment Concept & Solutions
- Vulnerability Assessment Tools & Reports



CoDING  
CREATROS