


NS3EDU.
Learn Today  Earn Tomorrow

CYBER SECURITY DIPLOMA



TABLE OF CONTENT

1	Overview	3
2	Roadmap of Job Placements	4
3	USP's	5
4	Course Outline	6 - 16
5	Our Placement Partner	18



NS3EDU: BRIDGE YOUR IT DREAMS TO REALITY



EMPOWERING CAREERS THROUGH KNOWLEDGE

Looking to make it big in the world of IT networking? Look no further than NS3Edu! We help beginners learn the ropes & experienced pros master new skills. Come join us and build your dream career!



MISSION

The mission of NS3Edu is to empower our candidates with in-depth knowledge of IT fundamentals along with real-time industry experience and also take 100% responsibility for the placement by making them Industry fit.

CERTIFICATES



VISION

In-depth knowledge + hands-on experience + analytical thinking = placement



Learning



Opportunity



Experience



Career



ROADMAP OF **JOB** PLACEMENT

Confused
in **Different**
Career Options



Qualifies-
Job Placement



Counselling &
Demo sessions



Opportunities
for **Job**
Placement



Student
Enrollment &
Induction
session



Screening by
Corporate **HR &**
Tech Team



Course
Kick off
(Live Classes)



2 Week **Technical**
Task Training



Access to
Recorded Sessions,
E book & Lab Manual



NS3 Tech
Industrial Exposure



Course Completion



Learning



Opportunity



Experience



Career

WHAT MAKES US UNIQUE?

USP's



NETWORKING ASSOCIATE

COURSE OUTLINE

Module-1

1. General Networking

- Introduction to Networks
- OSI Reference Model
- Ethernet Technologies
- Hubs vs Switches vs Routers
- IPv4 Addressing and Subnetting
- IPv6 Addressing
- TCP & UDP
- Introduction to 802.11 Wireless
- Cisco 802.11 Implementations

2. CCNA

Network Fundamentals

- Explain the role and function of network components
- Describe characteristics of network topology architectures
- Compare physical interface and cabling types
- Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting
- Describe the need for private IPv4 addressing
- Configure and verify IPv6 addressing and prefix
- Compare IPv6 address types
- Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- Describe wireless principles
- Explain virtualization fundamentals (virtual machines)



Network Fundamentals

- Configure and verify VLANs (normal range) spanning multiple switches
- Configure and verify inter switch connectivity
- Password Recovery And Switch Reset (Layer2/Layer 3)
- Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
- Upgradation of the Firmware's for Layer 2 and Layer 3 Switches through TFTP and USB
- Compare Cisco Wireless Architectures and AP modes
- Factory Reset of Access Points and Basic Ap Configuration
- Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports and LAG)
- Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)
- Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

IP Connectivity

- Interpret the components of routing table
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing
- Configure and verify single area OSPFv2
- Describe the purpose of first hop redundancy protocol

Security Fundamentals

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives (multi factor authentication, certificates, and biometrics)
- Describe remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Differentiate authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure WLAN using WPA2 PSK using the GUI
- Converting an AP from Mobility Express to CAPWAP Type and Vice Versa
- Configuration of AP as a Controller
- WLAN Configuration Cisco Mobility Express Controller with (WPA,WPA2,WPA3, Guest WLAN)

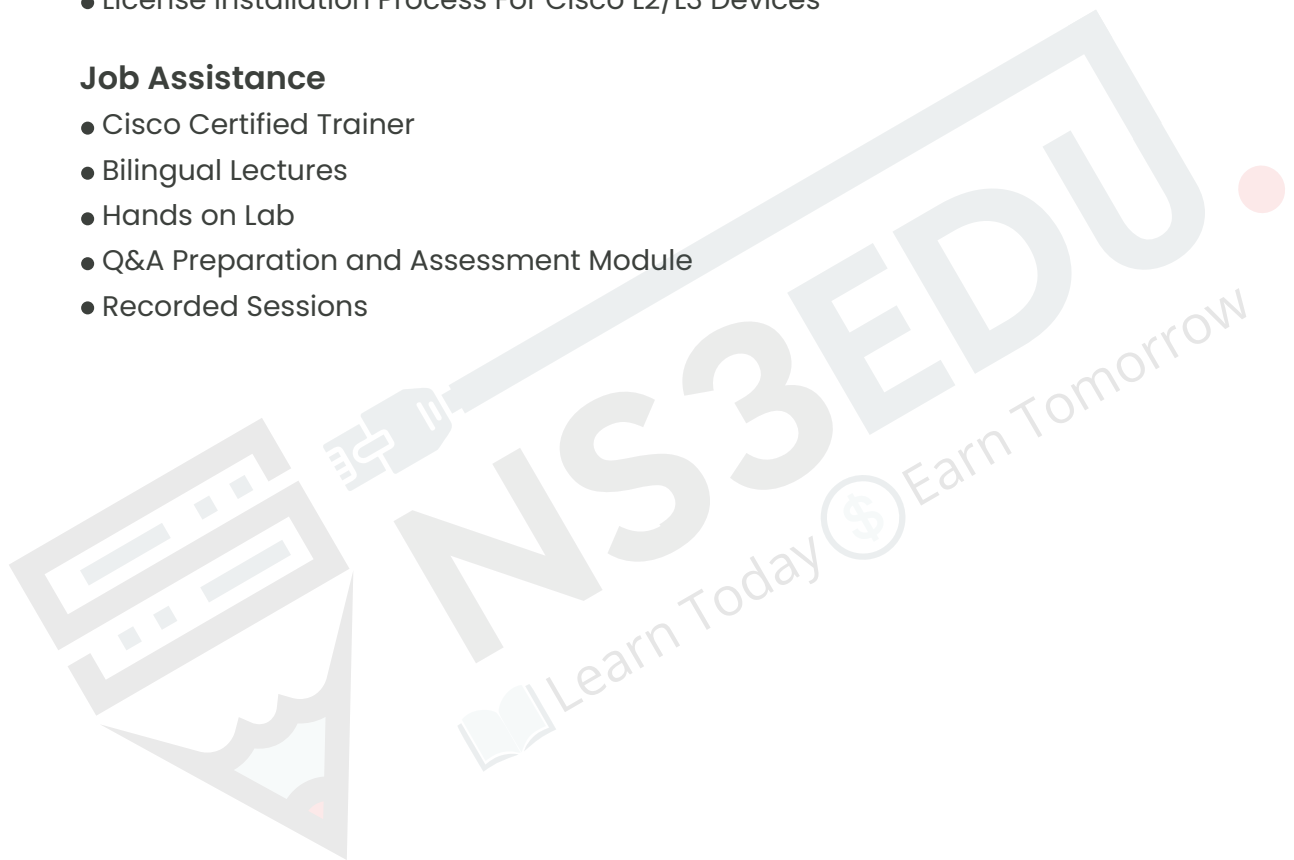


Automation & Programmability

- Explain how automation impacts network management
- Compare traditional networks with controller-based networking
- Describe controller-based and software defined architectures (overlay, underlay, and fabric)
- Compare traditional campus device management with Cisco DNA Center enabled device management
- Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
- Recognize the capabilities of configuration management mechanisms Puppet Chef & Ansible
- Interpret JSON encoded data
- License Installation Process For Cisco L2/L3 Devices

Job Assistance

- Cisco Certified Trainer
- Bilingual Lectures
- Hands on Lab
- Q&A Preparation and Assessment Module
- Recorded Sessions



Module-1 Exam

LINUX COURSE OUTLINE

Module-2

1) Linux Introduction

- What is Linux
- Why Linux
- Linux vs Windows
- CLI vs GUI

2) Distribution of Linux

- Types of Linux
- Different edition of Linux

3) Lab-setup & (errors-fix)

- VMware vs Virtual box
- Installation of VMware
- Licensing
- Interface setting's

4) Linux Interface

- Introduction to Linux interface
- Difference B/W Linux UI & Windows UI
- Setting up tools and other packages
- Getting familiar with Linux

5) Access command line

- What is Terminal
- Types of Terminal
- Setting up Terminal
- Learning Basic commands For CLI
- Top 100 Commands

6) Linux directory structure

- Understanding Linux Directory Structure
- Absolute path VS Relative path
- Getting familiar with Root Directory



7) Moving around directories

- Moving around via GUI & CLI
- Accessing Restricted files & directories

8) Create,view,edit text files via command line

9) Manage files from terminal

10) Getting help in linux

- Troubleshooting Common Linux Problem

11) Managing users in Linux

- Who is Root User
- Who is Service User
- Create user using Terminal
- Delete user's using Terminal
- Modify user using Terminal
- What is passwd file
- How to open Passwd file?

12) Managing groups in Linux

- What are Groups?
- Create Groups
- Delete Groups
- Set up Group Password

13) File permission

- How to access File Permission
- Understanding Linux file Permission
- Changing File permission
- Changing File Owner

14) Operators used in command line

- What are Operators
- Why are Operators used for?

Module-2 Exam



CERTIFIED ETHICAL HACKER COURSE OUTLINE

Module-3

Week 01 – Introduction to Ethical Hacking

- Lesson 01 – Information Security Overview
- Lesson 02 – Information Security Threats and Attack Vectors
- Lesson 06 – Penetration Testing Concepts
- Lesson 03 – Hacking Concepts
- Lesson 04 – Ethical Hacking Concepts
- Lesson 05 – Information Security Controls
- Lesson 07 – Information Security Laws and Standards

Week 02 – Footprinting and Reconnaissance

- Lesson 01 – Information Security Overview
- Lesson 02 – Information Security Threats and Attack Vectors
- Lesson 06 – Penetration Testing Concepts
- Lesson 03 – Hacking Concepts
- Lesson 04 – Ethical Hacking Concepts
- Lesson 05 – Information Security Controls
- Lesson 07 – Information Security Laws and Standards

Week 03 – Scanning Networks

- Lesson 01 – Network Scanning Concepts
- Lesson 02 – Scanning Tools
- Lesson 03 – Scanning Techniques
- Lesson 04 – Scanning Beyond IDS and Firewall
- Lesson 05 – Banner Grabbing
- Lesson 06 – Draw Network Diagrams
- Lesson 07 – Scanning Pen Testing



Week 04 – Enumeration

- Lesson 01 – Enumeration Concepts
- Lesson 02 – NetBIOS Enumeration
- Lesson 03 – SNMP Enumeration
- Lesson 04 – LDAP Enumeration
- Lesson 05 – NTP Enumeration
- Lesson 06 – SMTP Enumeration and DNS Enumeration
- Lesson 07 – Enumeration Countermeasures
- Lesson 08 – Other Enumeration Techniques
- Lesson 09 – Enumeration Pen Testing

Week 05 – Vulnerability Analysis

- Lesson 01 – Vulnerability Assessment Concepts
- Lesson 02 – Vulnerability Assessment Solutions
- Lesson 03 – Vulnerability Scoring Systems
- Lesson 04 – Vulnerability Assessment Tools
- Lesson 05 – Vulnerability Assessment Reports

Week 06 – System Hacking

- Lesson 01 – System Hacking Concepts
- Lesson 02 – Cracking Passwords
- Lesson 03 – Escalating Privileges
- Lesson 04 – Executing Applications
- Lesson 05 – Hiding Files
- Lesson 06 – Covering Tracks
- Lesson 07 – Penetration Testing



Week 07 – Malware Threats

- Lesson 01 – Malware Concepts
- Lesson 02 – Trojan Concepts
- Lesson 03 – Virus and Worm Concepts
- Lesson 04 – Malware Analysis
- Lesson 05– Countermeasures
- Lesson 06– Anti-Malware Software
- Lesson 07– Malware Penetration Testing

Week 08 – Sniffing

- Lesson 01– Sniffing Concepts
- Lesson 02– Sniffing Technique: MAC Attacks
- Lesson 03– Sniffing Technique: DHCP Attacks
- Lesson 04– Sniffing Technique: ARP Poisoning
- Lesson 05– Sniffing Technique: Spoofing Attacks
- Lesson 06– Sniffing Technique: DNS Poisoning
- Lesson 07– Sniffing Tools
- Lesson 08– Countermeasures
- Lesson 09– Sniffing Detection Techniques
- Lesson 10– Sniffing Pen Testing

Week 09– Social Engineering

- Lesson 01 – Social Engineering Concepts
- Lesson 02 – Social Engineering Techniques
- Lesson 03– Insider Threats
- Lesson 04 – Impersonation on Social Networking Sites
- Lesson 05 – Identity Theft
- Lesson 06 – Countermeasures
- Lesson 07 – Social Engineering Penetration Testing

Week 10- Denial-of-Service

- Lesson 01 - DoS/DDoS Concepts
- Lesson 02 - DoS/DDoS Attack Techniques
- Lesson 03 - Botnets
- Lesson 04 - DDoS Case Study
- Lesson 05 - DoS/DDoS Attack Tools
- Lesson 06 - Countermeasures
- Lesson 07 - DoS/DDoS Protection Tools
- Lesson 08 - DoS/DDoS Attack Penetration Testing

Week 11- Session Hijacking

- Lesson 01- Session Hijacking Concepts
- Lesson 02- Application Level Session Hijacking
- Lesson 03- Network Level Session Hijacking
- Lesson 04- Session Hijacking Tools
- Lesson 05- Countermeasures
- Lesson 06- Penetration Testing

Week 12 - Evading IDS, Firewalls & Honeypots

- Lesson 01- IDS, Firewall, and Honeypot Concepts
- Lesson 02- IDS, Firewall, and Honeypot Solutions
- Lesson 03- Evading IDS
- Lesson 04- Evading Firewalls
- Lesson 05- IDS/Firewall Evading Tools
- Lesson 06- Detecting Honeypots
- Lesson 07- IDS/Firewall Evasion Countermeasures
- Lesson 08- Penetration Testing

Week 13- Hacking Web Servers

- Lesson 01- Web Server Concepts
- Lesson 02- Web Server Attacks
- Lesson 03- Web Server Attack Methodology
- Lesson 04- Web Server Attack Tools
- Lesson 05- Countermeasures
- Lesson 06- Patch Management
- Lesson 07- Web Server Security Tools
- Lesson 08- Web Server Pen Testing

Week 14- Hacking Web Applications

- Lesson 01 - Web App Concepts
- Lesson 02 - Web App Threats
- Lesson 03 - Hacking Methodology
- Lesson 04 - Web Application Hacking Tools
- Lesson 05 - Countermeasures
- Lesson 06 - Web App Security Testing Tools
- Lesson 07 - Web App Pen Testing

Week 15- SQL Injection

- Lesson 01 - SQL Injection Concepts
- Lesson 02 - Types of SQL Injection
- Lesson 03 - SQL Injection Methodology
- Lesson 04 - SQL Injection Tools
- Lesson 05 - Evasion Techniques
- Lesson 06 - Countermeasures

Week 16- Hacking Wireless Networks

- Lesson 01 - Wireless Concepts
- Lesson 02 - Wireless Encryption
- Lesson 03 - Wireless Threats
- Lesson 04 - Wireless Hacking Methodology
- Lesson 05 - Wireless Hacking Tools
- Lesson 06 - Bluetooth Hacking
- Lesson 07 - Countermeasures
- Lesson 08 - Wireless Security Tools
- Lesson 09 - Wi-Fi Pen Testing

Week 17- Hacking Mobile Platforms

- Lesson 01- Mobile Platform Attack Vectors
- Lesson 02- Hacking Android OS
- Lesson 03- Hacking iOS
- Lesson 04- Mobile Spyware
- Lesson 05- Mobile Device Management
- Lesson 06- Mobile Security Guidelines and Tools
- Lesson 07- Mobile Pen Testing

Week 18- IoT Hacking

- Lesson 01- IoT Concepts
- Lesson 02- IoT Attacks
- Lesson 03- IoT Hacking Methodology
- Lesson 04- IoT Hacking Tools
- Lesson 05- Countermeasures
- Lesson 06- IoT Pen Testing

Week 19- Cloud Computing

- Lesson 01 - Cloud Computing Concepts
- Lesson 02 - Cloud Computing Threats
- Lesson 03 - Cloud Computing Attacks
- Lesson 04 - Cloud Security
- Lesson 05 - Cloud Security Tools
- Lesson 06 - Cloud Penetration Testing

Week 20- Cryptography

- Lesson 01- Cryptography Concepts
- Lesson 02- Encryption Algorithms
- Lesson 03- Cryptography Tools
- Lesson 04- Public Key Infrastructure (PKI)
- Lesson 05- Email Encryption
- Lesson 06- Disk Encryption
- Lesson 07- Cryptanalysis
- Lesson 08- Countermeasures

Module-3 Exam

EMPLOYABILITY SKILLS

PD Classes

Resume Building

Technical Workshops

Linkedin Classes

Q/A Prepration

Hands on Practice with Advance Devices

Mock Interview rounds with HR & Tech Team

Internship Opportunities



OUR PLACEMENT PARTNERS



Learning



Opportunity



Experience



Career

ACHIEVEMENTS



GURUGRAM(H.O)

B9, 3rd Floor, 302, Block B,
Old DLF, Sector 14, Gurugram
Haryana

+91 8800011138
info@ns3edu.com

LUCKNOW

Office space 1, First Floor Omaxe
Avenue Near Omaxe City
Bijnor Rd, Lucknow

+91 7703030320
info_lko@ns3edu.com

DELHI(BADARPUR)

Property No:-3, 3rd Floor Main
Mathura road nearby Badarpur
Police Station, Ch. Dharamvir
Market Badarpur New Delhi 110044

+91 7428080999
info_bpb@ns3edu.com



 www.ns3edu.com

 +91 8800 0111 38

Follow us for **Job Placement** & Knowledge updates

