CYBEREDU

TABLE OFCONTENTS

01. NETWORKING

Network deep study is crucial for CEH (Certified Ethical Hacker) because understanding the intricacies of network architecture, protocols, and traffic analysis enables ethical hackers to identify vulnerabilities and security weaknesses more effectively. In-depth knowledge of networking concepts such as TCP/IP, DNS, DHCP, and routing helps in detecting, analyzing, and mitigating network-based attacks. It also allows CEH professionals to simulate real-world attack scenarios, conduct thorough penetration testing, and implement robust security measures. Ultimately, a deep understanding of networks enhances an ethical hacker's ability to defend against sophisticated cyber threats and ensure comprehensive security assessments.

A. WEEK 1: NETWORKING BASICS & OSI MODEL

- Introduction to Networking Concepts
- Overview of OSI & TCP/IP Models
- Network Protocols: HTTP/S, FTP, ARP, ICMP, DNS
- Difference between TCP and UDP
- Introduction to Cisco Packet Tracer for Labs
- Lab: Simulate Ping, DNS lookup, and TCP/UDP traffic
- Introduction to Networking Concepts
- Overview of OSI & TCP/IP Models
- Network Protocols: HTTP/S, FTP, ARP, ICMP, DNS
- Difference between TCP and UDP
- Introduction to Cisco Packet Tracer for Labs
- Lab: Simulate Ping, DNS lookup, and TCP/UDP traffic

B. WEEK 2: IP ADDRESSING & TOPOLOGIES

- IPv4 Addressing, Classes, Subnetting, CIDR
- Static vs Dynamic IP Configuration
- IP Address Calculations & VLSM
- Network Topologies: Star, Bus, Mesh, Hybrid
- Lab: IP Addressing Design in Packet Tracer

C. WEEK 3: SWITCHING, LAN, AND VLANS

- Switched Networks: MAC Address Tables, ARP
- LAN Concepts: Broadcast/Collision Domains
- VLAN Creation and Configuration
- VLAN Trunking and Inter-VLAN Routing
- Lab: Implement VLANs and Basic Switching

D. WEEK 4: ROUTING & ACCESS CONTROL

- Static vs Dynamic Routing
- Introduction to Routing Tables and RIB
- Routing Protocols: RIP, OSPF (Basic)
- Access Control Lists (ACLs): Standard vs Extended
- Lab: Configure ACLs and Static Routing

CYBEREDU

TABLE OFCONTENTS

E. WEEK 5: DHCP, DNS, VTP & REDUNDANCY

- DHCP Overview, Configuration, and Spoofing Concepts
- DNS Resolution Process and CEH Attack Scenarios
- VLAN Trunking Protocol (VTP) Concepts
- LAN Redundancy: STP, HSRP
- Lab: DHCP, DNS, and Redundant Gateway Design

F. WEEK 6: LINK AGGREGATION,WIRELESS & IP SCALING

- EtherChannel & Port Aggregation
- Introduction to Wireless LAN Architecture
- Wireless Security: WPA, WPA2, WPA3
- IP Scaling Techniques
- Lab: Configure EtherChannel and Wireless Network

G. WEEK 7: ADVANCED ROUTING - OSPF, EIGRP, BGP

- OSPF Concepts: Areas, LSAs, DR/BDR
- EIGRP Overview and Basic Setup
- Introduction to External BGP (EBGP)
- Practical Route Summarization
- Lab: Multi-protocol Routing Lab in Packet Tracer

H. WEEK 8: NETWORK SERVICES, SECURITY & AUTOMATION

- WAN Technologies: P2P, Broadband
- IP Services: NAT, PAT, VPN intro
- Firewall & IPS Concepts (Cisco ASA/Zone-Based)
- Network Monitoring Tools: SNMP, NetFlow, Syslog
- Intro to SDN, Control Plane vs Data Plane
- Automation: CLI vs Controller (Cisco DNA, REST APIs)
- Lab: Full Network Build & Security Validation in Packet Tracer

I. TOOLS AND PLATFORMS REQUIRED:

- Cisco Packet Tracer (latest version)
- Optional: GNS3 or EVE-NG (for advanced setups)
- Wireshark (packet capture)
- Practice Labs from TryHackMe, Hack The Box (network-specific rooms)

CYBEREDU

TABLE OFCONTENTS

02 CEH-FOCUSED LINUX SYLLABUS (2 MONTHS)

Linux is important for CEH (Certified Ethical Hacker) because it provides a powerful, flexible, and open-source operating system environment that is essential for cybersecurity testing, penetration testing, and ethical hacking. Its widespread use in servers, networks, and security tools makes familiarity with Linux crucial for effective vulnerability assessment, exploitation, and security analysis. Learning Linux enables CEH professionals to leverage a vast array of security tools (like Kali Linux, Wireshark, Nmap, Metasploit) efficiently, understand underlying system behaviors, and develop custom scripts or exploits, thereby enhancing their overall hacking and defense capabilities.

A. WEEK 1: LINUX FUNDAMENTALS FORHACKERS

- Introduction to Linux distributions used in hacking (Kali, Parrot)
- Basic shell commands: ls, cd, pwd, cp, mv, rm, mkdir, touch
- File navigation and text editing with nano, vim
- User and group management: whoami, id, adduser, passwd
- File permissions: chmod, chown, umask

B. WEEK 2: SYSTEM MANAGEMENT & FILE OPERATIONS

- Directory structure and filesystem hierarchy (/etc, /bin, /home, /var, etc.)
- Package management: apt, dpkg, snap
- Disk management: df, du, mount, umount
- Working with cron and at for task scheduling
- Log files: /var/log/syslog, /var/log/auth.log, etc.

C. WEEK 3: NETWORKING ESSENTIALS

- Basic networking commands: ifconfig, ip, ping, netstat, ss
- Port scanning with nmap
- Network monitoring tools: tcpdump, wireshark, iftop
- DNS queries: dig, nslookup, host
- SSH and remote access: ssh, scp, sftp

D. WEEK 4: BASH SCRIPTING FOR ETHICAL HACKING

- Writing basic bash scripts
- Variables, conditionals (if, else), loops (for, while)
- Parsing text: grep, awk, sed, cut
- Automating scanning tasks and log parsing
- Script obfuscation basics

CYBEREDU

TABLE OFCONTENTS

E. WEEK 5: CEH TOOLSET SETUP AND USAGE

- Installing and using tools on Kali Linux:
  - nmap, nikto, dirb
  - hydra, john, hashcat
  - netcat, nc
- Using Metasploit basics: starting, modules, scanning
- Fileless malware handling & payloads with msfvenom
- Configuring iptables and basic firewall rules

F. WEEK 6: SYSTEM SECURITY AND HARDENING

- Understanding /etc/shadow, /etc/passwd structure
- Detecting unauthorized access and users
- Host-based firewalls (UFW)
- SSH hardening and disabling root login
- Password cracking techniques and defenses

G. WEEK 7: PRIVILEGE ESCALATION TECHNIQUES

- SUID/SGID binaries
- Kernel exploits (intro)
- Using sudo, su, and exploiting misconfigurations
- Finding privilege escalation vectors using linPEAS, Linux Exploit Suggester

H. WEEK 8: PRACTICE AND REAL-WORLD SCENARIOS

- Simulating attacks in a controlled lab (e.g., VulnHub or TryHackMe Linux boxes)
- Capture-the-Flag (CTF) challenges involving Linux
- Reporting findings (logs, screenshots, commands)
- Final assessment and recap

I. 🔧 TOOLS AND PLATFORMS REQUIRED:

- Kali Linux or Parrot OS (VirtualBox or native)
- VS Code or any terminal-based editor
- Access to labs like TryHackMe, Hack The Box, or CyberSecLabs

CYBEREDU

TABLE OFCONTENTS

3. 🧰 CEH V13 SYLLABUS: 20 MODULES 3-MONTH

CEH v13 with AI is the latest evolution in ethical hacking certification, combining foundational cybersecurity skills with cutting-edge AI-driven techniques. It equips learners to think like attackers, covering real-world hacking tools, Linux and networking essentials, and modern threats across cloud, mobile, and IoT environments. With 20 comprehensive modules and hands-on labs, CEH v13 prepares professionals to detect, analyze, and defend against cyberattacks using both traditional and AI-powered approaches.

A. 🔹 MONTH 1: FOUNDATIONS & CORE ATTACKS

Week 1: Introduction + Reconnaissance

- 🟦Module 1: Introduction to Ethical Hacking
- InfoSec concepts, hacking phases, legal aspects
- Information security controls & standards.

- 🟦Module 2: Footprinting and Reconnaissance
- Passive & active recon, Google hacking, WHOIS, DNS, social engineering.
- 🧪 Lab: WHOIS & DNS enumeration, OSINT using tools like Maltego, Recon-ng

Week 2: Scanning & Enumeration

- 🟦Module 3: Scanning Networks
- Port scanning, ping sweeps, banner grabbing

- 🟦Module 4: Enumeration
- NetBIOS, SNMP, LDAP, NTP, DNS enumeration
- 🧪 Lab: Nmap scans, NetBIOS/SMB enumeration using enum 4linux & SNMPwalk

Week 3: Vulnerabilities + System Hacking

- 🟦Module 5: Vulnerability Analysis
- Vulnerability scanning tools (Nessus, OpenVAS), CVEs

- 🟦Module 6: System Hacking
- Password cracking, privilege escalation, maintaining access
- 🧪 Lab: Password attacks (Hydra, John), privilege escalation techniques

Week 4: Malware + Sniffing

- 🟦Module 7: Malware Threats
- Types: Trojans, viruses, worms, ransomware

- 🟦Module 8: Sniffing
- MITM attacks, ARP spoofing, sniffing tools (Wireshark, Ettercap)
- 🧪 Lab: Packet capture analysis, MITM via ARP spoofing

TABLE OF CONTENTS

B. MONTH 2: ATTACKS ON NETWORKS, SYSTEMS & WEB

- Week 5: Social Engineering + DoS

- 🟦Module 9: Social Engineering
- Phishing, pretexting, impersonation, USB drops

- 🟦Module 10: Denial-of-Service
- DoS/DDoS, botnets, LOIC, HOIC
- 🧪 Lab: Phishing simulation (Social-Engineer Toolkit), DoS in lab setup

Week 6: Session Hijacking + Evasion

- 🟦Module 11: Session Hijacking
- TCP session hijacking, cookie hijacking, countermeasures

- 🟦Module 12: Evading IDS, Firewalls & Honeypots
- IDS/IPS evasion, packet fragmentation, tunneling
- 🧪 Lab: Hijack sessions using tools like Bettercap, evade Snort rules

Week 7: Web Server & Web App Hacking

- 🟦Module 13: Hacking Web Servers
- Exploiting IIS, Apache, web server misconfigurations

- 🟦Module 14: Hacking Web Applications
- OWASP Top 10, XSS, CSRF, directory traversal
- 🧪 Lab: Exploits using DVWA, Burp Suite, OWASP Juice Shop

Week 8: SQL Injection + Wireless Attacks

- 🟦Module 15: SQL Injection
- In-band, out-of-band, blind injection, evasion

- 🟦Module 16: Hacking Wireless Networks
- Wi-Fi encryption (WEP, WPA2), evil twin, cracking techniques
- 🧪 Lab: SQLi with sqlmap, WPA2 cracking using aircrack-ng

CYBEREDU

TABLE OFCONTENTS

C. MONTH 3: ADVANCED PLATFORMS, CLOUD & CRYPTO

Week 9: Mobile + IoT/OT Hacking

- 🟦Module 17: Hacking Mobile Platforms
- Mobile OS architecture, malware analysis, mobile exploits

- 🟦Module 18: IoT and OT Hacking
- SCADA/ICS basics, MQTT, IoT footprinting, vulnerabilities
- 🧪 Lab: Android APK reverse engineering, Shodan-based IoT recon

Week 10: Cloud + Cryptography

- 🟦Module 19: Cloud Computing
- Cloud security threats, containers, serverless, identity management

- 🟦Module 20: Cryptography
- Symmetric/asymmetric encryption, hashing, PKI, attacks (rainbow tables, MITM)
- 🧪 Lab: Encrypt/decrypt using GPG, hash cracking with hashcat

Week 11: Practice Labs + Simulations

- 🥷 Simulated attacks across domains: network, web, system
- 🧪 Practice labs: Metasploit, CTF-style exercises on TryHackMe/VulnHub
- 📊 Group assignment: Write a sample pentest report

Week 12: Review + Exam Prep

- 🧠 Recap all modules with flashcards, quizzes, cheat sheets
- 🧪 Mock tests (CEH practice exam format)
- 📋 Final CTF challenge or lab walkthrough
- 🎯 Certification tips, real-world application overview

🔧 Tools & Platforms Used:

- Kali Linux, Metasploit, Nmap, Burp Suite, Wireshark, Aircrack-ng, Hydra, SQLmap, John the Ripper
- TryHackMe, Hack The Box, VirtualBox/Vmware, DVWA, OWASP Juice Shop