HACKSTRIX CERTIFIED NETWORKING ESSENTIALS

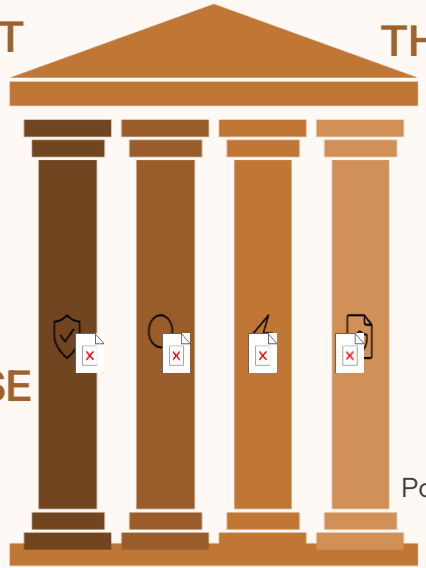
FOR CYBERSECURITY PROFESSIONALS

RISK ASSESSMENT

Identify and prioritize threats

THREAT DETECTION

Monitor and detect intrusions promptly



INCIDENT RESPONSE

Contain, eradicate, and recover fast

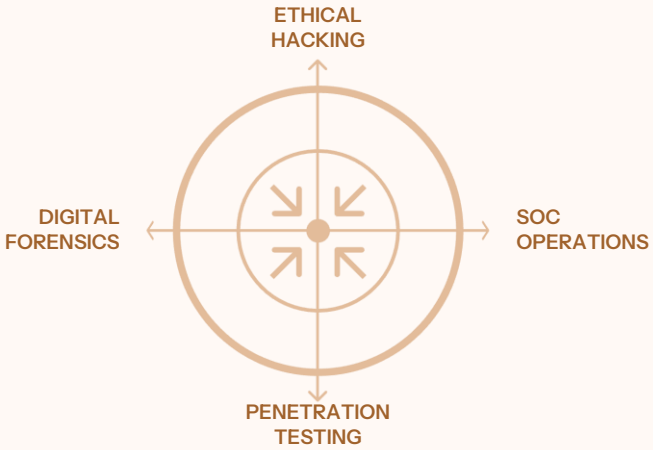
SECURITY GOVERNANCE

Policies, training, and compliance

COURSE OVERVIEW

WHO IS THIS FOR?

This course is designed for beginners and aspiring cybersecurity professionals who want to build strong networking fundamentals required for ethical hacking, SOC operations, penetration testing, digital forensics, and system administration.



MODE: LIVE ONLINE

Live interactive sessions delivered in real-time, allowing direct engagement with instructors and peers

DURATION: 4 WEEKS

A focused, intensive program that takes you from beginner to intermediate networking competence in just four weeks

SKILL LEVEL: BEGINNER TO INTERMEDIATE

No prior networking experience required. The course builds your knowledge progressively, from foundational concepts to practical cybersecurity-focused networking skills. A certificate of completion is awarded upon finishing the program.

MODULES 1 & 2: NETWORKING FOUNDATIONS & MODELS

The first two modules lay the groundwork for everything that follows. You'll understand how networks function, how data moves across them, and how the industry's most critical reference models map to real-world attack surfaces.

MODULE 1: INTRODUCTION TO NETWORKING

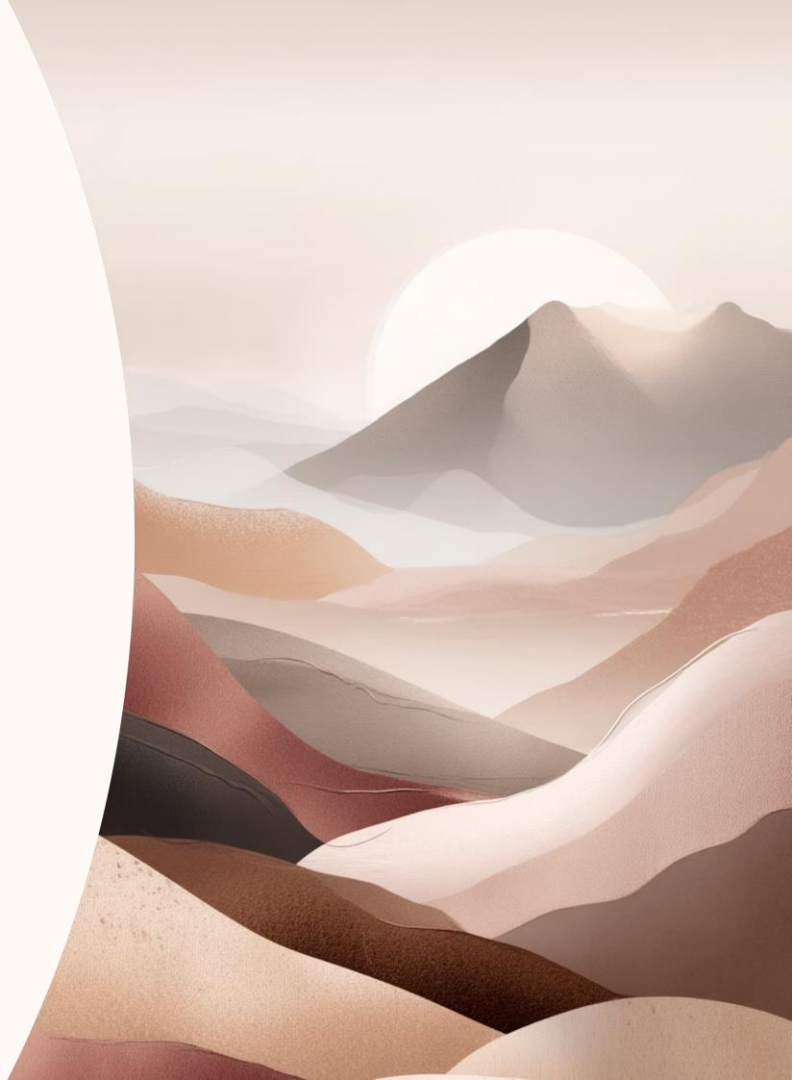
Cover the basics: types of networks (LAN, WAN, MAN, PAN), network topologies, client-server vs. peer-to-peer models, network devices, the role of networking in cybersecurity, and how data is transmitted across systems.

MODULE 2: OSI & TCP/IP MODELS

Explore the OSI 7-layer model and TCP/IP model in depth. Understand encapsulation and decapsulation, protocol functions at each layer, and critically—how each layer presents a distinct attack surface for cyber threats.

REAL-WORLD CONTEXT

Every concept is grounded in practical examples drawn from actual networking environments, helping you immediately connect theory to the scenarios you'll encounter in cybersecurity roles and penetration testing engagements.



CORE TECHNICAL SKILLS

MODULES 3 & 4: IP ADDRESSING, SUBNETTING & PROTOCOLS

These modules give you command over the language of the internet. From carving networks with subnetting to understanding the protocols that power every service you'll ever test or defend, this knowledge is the backbone of all cybersecurity work.

MODULE 3: IP ADDRESSING & SUBNETTING

Master IPv4 and IPv6 basics, public vs. private IPs, CIDR notation, subnet masks, subnetting concepts, and the roles of Gateway, DNS, and DHCP. Understand static vs. dynamic IP addressing in network design.

MODULE 4: NETWORK PROTOCOLS & SERVICES

Deep dive into the protocols every cybersecurity professional must know: HTTP/HTTPS, FTP/SFTP, DNS, DHCP, SSH, SMTP/POP3/IMAP, SNMP, ICMP, ARP, and SMB—understanding both their function and their vulnerabilities.

WHY THIS MATTERS FOR CYBERSECURITY

Understanding how protocols are designed—and where they break—is essential for identifying misconfigurations, crafting exploits, and building effective defenses. These modules form the technical core of the course.

MODULES 5 & 6: SWITCHING, ROUTING & WIRELESS NETWORKING

From how data flows within a local network to how wireless signals can be exploited, these two modules bridge the gap between physical infrastructure and the attack techniques used against it in real-world engagements.

SWITCHING & ROUTING ESSENTIALS

Understand MAC addressing, the switching process, VLAN basics, trunking concepts, routing fundamentals, static vs. dynamic routing, and NAT basics—the building blocks of any enterprise network.

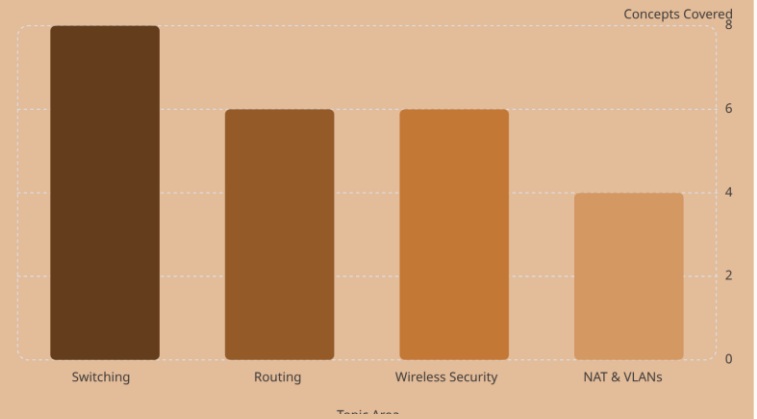
WIRELESS NETWORKING FUNDAMENTALS

Explore WiFi standards, wireless encryption methods, access points and controllers, wireless threats, and rogue access points. Learn WiFi security best practices critical for real-world assessments.

SECURITY RELEVANCE

VLANs, trunking misconfigurations, and rogue access points are among the most exploited weaknesses in enterprise environments. Understanding these is essential for any penetration tester or network defender.

SWITCHING VS. ROUTING VS. WIRELESS: COVERAGE



MODULE 7: NETWORK SECURITY FUNDAMENTALS

The dedicated security module brings together everything learned in the course and applies it directly to defending—and attacking—network infrastructure. This is where networking knowledge transforms into cybersecurity expertise.

DEFENSIVE TECHNOLOGIES

Learn how firewalls, IDS/IPS systems, VPNs, proxy servers, and access control lists work together to create layered network defenses. Understand network hardening principles used by security engineers.

COMMON NETWORK ATTACKS

Study the mechanics behind DDoS attacks, Man-in-the-Middle (MITM) attacks, and ARP spoofing. Understanding how these attacks are executed is essential for building effective countermeasures and detecting them in SOC environments.

PRACTICAL APPLICATION

Security concepts are tied directly to real threat scenarios. Students leave this module able to identify misconfigurations, recognize attack patterns, and recommend appropriate defensive controls for a given network environment.

MODULE 8 & TOOLS: MONITORING, TROUBLESHOOTING & HANDS-ON PRACTICE

1 NETWORK MONITORING & TROUBLESHOOTING

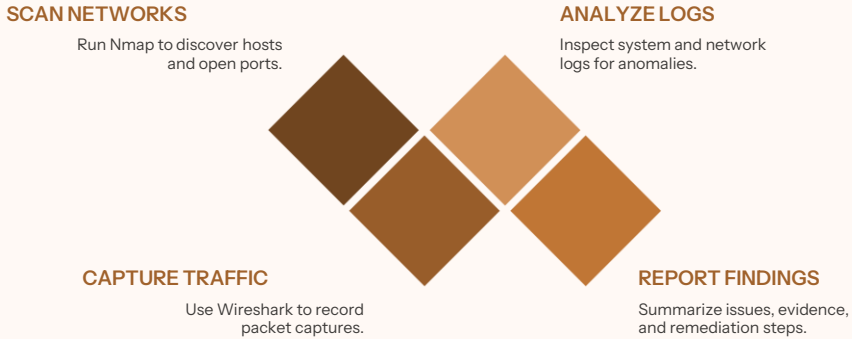
Use Ping, Traceroute, Netstat, Nslookup, and Dig for diagnostics. Learn port scanning basics, network performance monitoring, log analysis, and packet capture with Wireshark.

2 OFFENSIVE & RECON TOOLS

Get hands-on with Nmap, Angry IP Scanner, Netcat, and tcpdump—the tools used daily by penetration testers, SOC analysts, and network administrators worldwide.

3 PLATFORM & COMMAND LINE SKILLS

Work with PuTTY for remote access, Windows networking tools, and Linux networking commands. Build the cross-platform fluency every cybersecurity professional needs in the field.



The tools covered in this course—Wireshark, Nmap, tcpdump, Netcat, and more—are industry-standard instruments used in real penetration tests, SOC investigations, and digital forensics cases. You won't just learn about them; you'll use them.

CERTIFICATION & ENROLMENT

EARN YOUR HCNEP CERTIFICATION & BEGIN YOUR JOURNEY

Upon completing the course, you will be awarded the **Hackstrix Certified Network Essentials Professional (HCNEP)** certification—a credential that validates your foundational networking expertise to employers, clients, and cybersecurity programs worldwide.

CONFIRM YOUR ELIGIBILITY

This course is open to complete beginners. No prior networking or cybersecurity experience is required—just a commitment to learning and a drive to build a career in cybersecurity.

ENROL & ATTEND LIVE SESSIONS

Join the live online interactive sessions over 4 weeks. Engage directly with instructors, ask questions in real-time, and collaborate with fellow aspiring cybersecurity professionals.

GET IN TOUCH

Contact us at **8796381043** or visit hackstrix.com to register, ask questions, and take the first step toward your cybersecurity career.

Build a strong networking foundation and start your cybersecurity journey with Hackstrix. Every expert was once a beginner. The HCNEP certification is your first step toward a career in ethical hacking, SOC operations, penetration testing, and beyond. Invest in your skills today—your future in cybersecurity starts here.