A Comprehensive Roadmap to Modern Cybersecurity Certifications: Foundational Skills, Ethical Hacking, Cloud Security, and Linux Mastery

Executive Summary: Navigating Your Cybersecurity Career Path

The landscape of cybersecurity demands a continuous evolution of skills and knowledge. Traditional IT certifications, while once foundational, have largely been superseded by specialized, hands-on, and cloud-integrated credentials. This report provides a detailed roadmap for individuals seeking to enter the cybersecurity field, focusing on modern prerequisites, ethical hacking, cloud security, and a deep understanding of Linux/Unix operating systems. The analysis emphasizes the critical shift towards performance-based validation and practical application, which is paramount for success in today's dynamic threat environment.

The recommendations outlined herein guide aspiring professionals through a structured learning journey, beginning with robust foundational networking and operating system expertise, progressing to specialized offensive security techniques, and culminating in advanced cloud security architecture. Each suggested certification is accompanied by a thorough breakdown of its curriculum, the integration of practical laboratory exercises, and available written materials, ensuring a comprehensive and actionable learning path. The report underscores that the industry now values demonstrable, specialized skills, particularly in cloud environments and practical offensive/defensive techniques. This implies a need for recommendations that not only provide modern skills but also offer clear career progression paths, aligning with the dynamic nature of cybersecurity.

Your Cybersecurity Journey: Modern Prerequisites and Learning Approaches

Transitioning from Outdated Certifications: What's Relevant Today

The cybersecurity field has undergone a significant transformation, rendering some previously sought-after certifications less relevant for current industry demands. For instance, the broad "Cisco Certified Network Architect" role has evolved into more specialized networking and security architecture paths. While Cisco certifications maintain high relevance, foundational networking is now typically addressed by the Cisco Certified Network Associate (CCNA), with deeper security-focused architectural roles covered by credentials like CCNP Security.[1]
Similarly, the "Microsoft Certified Service Engineer" has been replaced by role-based and cloud-specific certifications, particularly those centered on Microsoft Azure. Modern equivalents include the Microsoft Certified: Azure Administrator Associate (AZ-104) for general cloud service management and the Microsoft Certified: Azure Security Engineer Associate (AZ-500) for securing cloud services. The pinnacle for security design and strategy in the Microsoft ecosystem is the Microsoft Certified: Cybersecurity Architect Expert (SC-100).[3]
The concept of a "Critical Ethical Hacker" has also diversified into a spectrum of certifications, ranging from entry-level to highly advanced, all emphasizing practical penetration testing and ethical hacking methodologies. Key modern certifications in this domain include eJPT, CompTIA PenTest+, EC-Council CEH, and Offensive Security OSCP.[9] The industry's current trajectory highlights a strong preference for vendor-specific cloud expertise (e.g., Microsoft Azure), performance-based validation of skills, and specialized roles over generalized titles. Certifications are now more closely aligned with specific job functions and necessitate demonstrable hands-on abilities. The observation that previous certifications are considered outdated indicates a clear understanding of the need for current relevance. This suggests that the recommended learning paths must not only impart modern skills but also illustrate clear career progression, aligning with the fluid nature of cybersecurity roles.

The Power of Hands-on Learning: Theory Meets Practice

A critical requirement for aspiring cybersecurity professionals is the integration of theoretical knowledge with practical application. The demand for "guided practical applications and written sources lesson by lesson, for which after I do the theoretical reading part I can then apply on a chapter by chapter basis" is a central theme of this learning journey. This preference aligns perfectly with the industry's current emphasis on demonstrable, hands-on skills. Modern cybersecurity certifications are designed to ensure that candidates can actively perform tasks, not merely recall facts. This is a direct response to employer demand for individuals who possess the capability to execute job responsibilities effectively.
Many of the recommended courses intrinsically weave virtual labs, simulated environments, and scenario-based projects directly into their curriculum, often in conjunction with theoretical modules. This structural design facilitates the immediate application of learned

concepts, reinforcing understanding through practical engagement. The widespread adoption of hands-on labs across nearly all modern certifications—including Cisco, Microsoft, CompTIA, Offensive Security, INE, Red Hat, and LPI—is not merely a desirable feature but a fundamental transformation in cybersecurity education. This pervasive emphasis on practical experience reflects the reality that cybersecurity is an applied field where theoretical knowledge alone is insufficient. Effective cybersecurity professionals are developed through experiential learning, making the preference for practical application a strong indicator of potential success in this domain.

Table 1: Cybersecurity Certification Roadmap (Overview)

Certification Name	Domain	Level	Key Skills Gained	Estimated Duration	Key Learning Platform(s)
CompTIA Network+ (N10-009)	Networking	Foundational	Network concepts, infrastructure, operations, security, troubleshooting	Self-paced, ~90 hours	uCertify, New Horizons, CompTIA CertMaster
Cisco CCNA (200-301)	Networking	Associate	Network fundamentals, IP connectivity, security, automation, routing/switching	6-9 months (series)	Cisco Networking Academy, Cisco Press, Udemy
CompTIA Linux+ (XK0-005)	Operating Systems	Intermediate	Linux administration, security, scripting, containers, troubleshooting	Self-paced, ~6 months	CompTIA CertMaster, Dion Training, ONLC
Red Hat Certified System Administrator (RHCSA EX200)	Operating Systems	Intermediate	RHEL administration, file/user/storage management, security, networking	3-6 months (courses)	Red Hat Training, Global Knowledge, LabEx

LPIC-1 (101-500 & 102-500)	Operating Systems	Foundational	Linux command line, installation, package management, basic networking	Self-paced, ~3-5 months	LPI Official, uCertify
eJPT (eLearnSecurity Junior Penetration Tester)	Ethical Hacking	Entry-Level	Assessment methodologies, host/network auditing, pen testing, web app pen testing	Self-paced, ~150 hours	INE Penetration Testing Student Learning Path, TryHackMe
CompTIA PenTest+ (PT0-002)	Ethical Hacking	Intermediate	Pen test planning, info gathering, attacks, reporting, tools	Self-paced, ~3-4 months	Infosec Institute, Training Camp, e-Careers
EC-Council Certified Ethical Hacker (CEH v13)	Ethical Hacking	Intermediate	Ethical hacking methodologies, 550+ attack techniques, AI integration	5 days (bootcamp), ~40 hours (self-study)	EC-Council Official Training, Infosec Institute
Offensive Security Certified Professional (OSCP PEN-200)	Ethical Hacking	Advanced	Practical pen testing, Kali Linux tools, exploitation, privilege escalation	3-6 months (course + lab)	Offensive Security Official, Firebrand Training
Microsoft Certified: Azure Administrator Associate (AZ-104)	Cloud Security	Intermediate	Azure identity, governance, storage, networking, compute, automation	3-6 months (specialization)	Microsoft Learn, Coursera (Packt), Learning Tree
Microsoft Certified: Azure Security Engineer Associate (AZ-500)	Cloud Security	Intermediate	Azure identity/access security, platform protection, data/app	6 months (professional cert)	Microsoft Learn, Coursera, Global Knowledge

			security, SecOps		
Microsoft Certified: Cybersecurity Architect Expert (SC-100)	Cloud Security	Expert	Zero Trust design, GRC, SecOps, data/app security, hybrid/multi-cloud	Advanced	Microsoft Learn

Foundational Networking Skills for Cybersecurity

Understanding how networks operate is an indispensable prerequisite for any cybersecurity professional. Without a solid grasp of networking principles, securing systems becomes an insurmountable challenge. This section addresses the interest in "Cisco certified Network Architect" by presenting modern, relevant pathways into networking.

CompTIA Network+ (N10-009): Building Your Network Backbone

CompTIA Network+ (N10-009) is a widely recognized, vendor-neutral certification that establishes a strong foundation in networking. This credential validates the essential skills required to troubleshoot, configure, and manage both wired and wireless networks, making it highly valued by global technology enterprises.[14]

The curriculum for CompTIA Network+ is structured to provide a comprehensive understanding of networking fundamentals. It covers core networking concepts, including a detailed comparison of the OSI and TCP/IP models to illustrate how data traverses networks, an identification of the role of each network layer in communication and troubleshooting, and an exploration of various network topologies such as star, mesh, and hybrid configurations. It also delves into transport layer protocols like TCP and UDP.[15] The course further examines network infrastructure, detailing the installation, termination, and testing of Ethernet cabling for reliable connectivity, alongside the configuration and deployment of Ethernet switches for optimal network performance. A significant portion is dedicated to IP addressing, covering IPv4, IPv6, and subnetting, as well as router configuration and troubleshooting.[15] Network operations are also a key focus, including common network services such as DHCP, DNS, and NAT, and how network applications like VoIP and web servers function. Performance monitoring and high availability mechanisms are also addressed.[15] Crucially for cybersecurity, the certification introduces fundamental network security concepts, including authentication, encryption, and firewalls, and how to support and troubleshoot secure network environments. Finally, it covers network troubleshooting and tools, encompassing the diagnosis of common network issues, disaster recovery, and business continuity planning.[14]

A significant advantage of CompTIA Network+ is its vendor-neutral nature.[14] This means that the foundational knowledge acquired is universally applicable across diverse hardware and software vendors. For individuals new to cybersecurity, this broad applicability is particularly beneficial, as it provides a versatile skill set that is not tied to a single product or company. Professionals with vendor-neutral skills are more adaptable and employable across various organizational environments, as they understand core principles that apply regardless of whether they encounter Cisco, Juniper, or other networking equipment. This broad conceptual framework serves as an excellent initial prerequisite, upon which more specialized, vendor-specific knowledge can be built.

The certification emphasizes interactive labs and practical application. Integrated labs provide a non-production, risk-free environment for hands-on experience, allowing learners to engage with simulated real-world scenarios.[14] These exercises include practical tasks such as installing and terminating Ethernet cabling, configuring switches, troubleshooting common Ethernet issues, configuring routers, deploying Wi-Fi networks, and implementing security controls.[15] Recommended learning resources include uCertify, which offers CompTIA Network+ Certification Training with over 50 interactive items, integrated labs, simulated scenarios, and immediate feedback in a flexible, self-paced format. Its materials are based on the official study guide, featuring diagrams and interactive questions designed for chapter-by-chapter theoretical reading followed by practical application.[14] New Horizons also provides expert-led, 5-day CompTIA Network+ training that covers designing, managing, and troubleshooting networks, with an optional exam voucher.[15] While not explicitly detailed for Network+ in all provided materials, CompTIA generally offers CertMaster Learn for self-paced study and CertMaster Labs for browser-based virtual labs across its certifications, which include extensive step-by-step activities aligned with exam objectives.[16] While CompTIA recommends prior CompTIA A+ certification and 9-12 months of experience as a junior network administrator or support technician, these are not mandatory prerequisites for the Network+ exam.[14]

Cisco Certified Network Associate (CCNA 200-301): The Industry Standard

The Cisco Certified Network Associate (CCNA 200-301) is an industry-recognized credential that validates expertise in a wide array of networking domains, including network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation. This certification is designed to prepare individuals for associate-level job roles such as Network Administrator, System Administrator, or Network Engineer.[1] It serves as a direct and highly relevant pathway for those interested in Cisco networking.

The CCNA curriculum is typically delivered through a comprehensive three-course series by Cisco Networking Academy. The first course, **CCNA: Introduction to Networks (ITN)**, lays the groundwork by covering network architectures, components, and topologies. It introduces

concepts of reliable networks, foundational network security, IP addressing (both IPv4 and IPv6), Ethernet principles, basic device configuration using Cisco IOS, and initial troubleshooting techniques.[1] Subsequent modules delve into the physical layer, data link layer, network layer, transport layer, and application layer, providing a holistic view of network communication.[1]

The second course, **CCNA: Switching, Routing, and Wireless Essentials (SRWE)**, builds upon these fundamentals by focusing on switching concepts, Virtual Local Area Networks (VLANs), and Inter-VLAN routing. It explores Spanning Tree Protocol (STP) and EtherChannel for network redundancy and performance. This course also covers DHCPv4/v6, First Hop Redundancy Protocols (FHRP), and crucial switch security measures, including port security and mitigation strategies against VLAN, DHCP, ARP, and STP attacks. Additionally, it provides a thorough understanding of Wireless Local Area Network (WLAN) concepts and configuration.[19]

The final course in the series, **CCNA: Enterprise Networking, Security, and Automation (ENSA)**, covers advanced topics such as OSPFv2, in-depth network security concepts (including threat actors, malware, common attacks, IP/TCP/UDP vulnerabilities, and cryptography), Access Control Lists (ACLs) for IPv4, Network Address Translation (NAT), and various Wide Area Network (WAN) technologies like VPN and IPsec. It also addresses Quality of Service (QoS), network management protocols (NTP, SNMP, Syslog), network design principles, advanced troubleshooting, network virtualization, and the burgeoning field of network automation, including Software-Defined Networking (SDN), APIs, REST, and configuration management tools.[21]

A key strength of the CCNA program lies in its extensive interactive labs and real-world scenarios. Cisco Networking Academy courses incorporate numerous interactive labs—for example, 90 labs in ITN and 47 labs in ENSA—to provide practical experience.[1] A cornerstone of this practical training is the use of

Cisco Packet Tracer, a network simulation tool. This tool allows learners to gain hands-on experience in building Local Area Networks (LANs), implementing network security measures, and configuring routers and switches in a virtual environment.[1] Official Cert Guides published by Cisco Press further enhance this practical learning by including free hands-on exercises and access to the

CCNA Network Simulator Lite software, which offers 34 free lab exercises designed to simulate actual Cisco routers and switches.[24] These labs cover essential topics such as configuring local usernames, hostnames, interface status, switch IP settings, Command Line Interface (CLI) configuration processes, passwords, and VLAN troubleshooting.[27]

The strategic use of Cisco Packet Tracer and Network Simulator Lite is a pedagogical choice that allows learners to experiment with complex network configurations and security measures in a risk-free, virtual environment. This approach effectively bridges the gap between theoretical knowledge and practical application without requiring expensive physical equipment. This removes significant financial and logistical barriers for aspiring professionals, democratizing practical networking education. Furthermore, the ability to easily reset and re-attempt labs makes chapter-by-chapter application of concepts highly feasible, aligning

perfectly with a learning style that prioritizes immediate practical reinforcement of theoretical understanding.

Recommended learning resources include the official three-course series from **Cisco Networking Academy**, which provides interactive content, practice labs, videos, and assessments.[1] The **Cisco Press Official Cert Guides (200-301)** are comprehensive review and practice packages, considered the only self-study resources approved by Cisco. These guides are meticulously structured chapter-by-chapter, covering all exam topics in detail.[24] Additionally, platforms like Udemy offer various CCNA courses, often including hands-on lab exercises, flashcards, quizzes, and practice exams, with some courses even featuring videos demonstrating real Cisco equipment.[18] While there are no formal prerequisites for the CCNA exam, a foundational understanding of networking concepts is highly beneficial.[1]

Table 2: Networking Certifications Comparison

Certification Name	Vendor	Level	Vendor-Neutral/Specific	Key Focus Areas	Hands-on Lab Environment	Typical Learning Resources	Recommended Prerequisites
CompTIA Network+ (N10-009)	CompTIA	Foundational	Vendor-Neutral	Network concepts, infrastructure, operations, security, troubleshooting	Integrated virtual labs, simulated scenarios	uCertify, New Horizons, CompTIA CertMaster Learn + Labs	CompTIA A+, 9-12 months network experience (recommended)
Cisco CCNA (200-301)	Cisco	Associate	Vendor-Specific (Cisco)	Network fundamentals, IP connectivity, IP services, security, automation, routing/switching	Cisco Packet Tracer, Network Simulator Lite, interactive labs	Cisco Networking Academy, Cisco Press Official Cert Guides, Udemy	No formal prerequisites (foundational networking beneficial)

Mastering Operating Systems: Linux/Unix for Cybersecurity Professionals

A deep understanding of Linux/Unix operating systems is a fundamental skill in cybersecurity, as many servers, specialized security tools (such as Kali Linux), and modern cloud environments are built upon these platforms. The request to "really help me get to learn and understand about operating systems such as linux/unix based and really get me to learn and interact with them" highlights this critical need.

CompTIA Linux+ (XK0-005): Vendor-Neutral Linux Competence

CompTIA Linux+ (XK0-005) is a highly respected, vendor-neutral professional certification that validates a high level of proficiency in using Linux within a business environment.[16] It specifically focuses on the foundational skills necessary for supporting Linux systems in an early career stage.[31]

The curriculum for CompTIA Linux+ is comprehensive, covering four key domains. **System Management** delves into Linux fundamentals, including filesystem hierarchy, the basic boot process, kernel panic scenarios, and device types. It also covers file and directory management (editing, compression, archiving, metadata, links, copying between systems), storage configuration (disk partitioning, Logical Volume Manager (LVM), RAID inspection, Storage Area Network (SAN)/Network-Attached Storage (NAS)), process and service management, and networking tools. Furthermore, it addresses software installation and management using package managers like DNF and APT, and general configuration management.[30]

Security is a significant component, focusing on best practices such as Public Key Infrastructure (PKI) certificates, authentication methods, Linux hardening techniques, identity management (account creation and deletion), firewall configuration, SELinux or AppArmor implementation, logging services, and data backup/restore procedures.[30]

The certification also includes a forward-looking domain on **Scripting, Containers, and Automation**. This section teaches how to create simple shell scripts (specifically Bash) to automate common tasks, perform basic container operations and image management, and utilize version control with Git (clone, push, pull, commit, add, checkout, branch, tag, gitignore). It also introduces Infrastructure as Code (IaC) technologies and concepts related to Kubernetes, container networks, and service meshes.[31] The inclusion of scripting, containers, and automation within CompTIA Linux+ reflects the modern DevOps and cloud-native landscape in IT. This indicates that contemporary Linux administration extends beyond managing individual servers to encompass automating tasks and understanding containerized environments, which are crucial for scalable and secure deployments in cybersecurity. This prepares professionals for environments where efficient and consistent

security configurations are paramount, and where misconfigurations in automated or containerized systems can introduce significant vulnerabilities.
Finally, **Troubleshooting** is a core domain, covering issues related to storage (latency, throughput, IOPS, capacity, filesystem, I/O scheduler, device, mount options), network resources (configuration, firewall, interface errors, bandwidth, name resolution), CPU and memory (runaway processes, high utilization, memory exhaustion), and user-related problems (login, file access, passwords, privilege elevation, quotas). It also teaches how to use system tools for diagnosing and resolving common Linux system problems.[31]
CompTIA Linux+ offers robust hands-on labs and practical exercises. **CompTIA CertMaster Labs for Linux+ (XK0-005)** provides browser-based virtual labs that simulate real IT environments, enabling users to configure operating systems, troubleshoot networks, and manage users and workstations.[17] These labs feature extensive, step-by-step activities directly aligned with the exam objectives.[17] Additionally, the
Dion Training Practice Lab offers simulated hands-on experience in managing, configuring, and maintaining Linux operating systems through 24 modules and exercises covering installation, file and directory management, text editing (Vi, Vim, Nano), access control, backup and compression, package management (DNF, APT), and remote access via SSH.[37]
Recommended learning resources include the **Official CompTIA Student Guides/eBooks**, which are rigorously evaluated to cover all exam objectives and impart knowledge and skills for both on-premises and cloud-based Linux server environments.[33] Comprehensive bundles like
CompTIA CertMaster Learn + Labs offer self-paced study with integrated virtual labs.[16]
ONLC Training Centers provides an on-demand, self-study course that includes digital materials, videos, practice questions, and virtual machine labs.[30] Learning Tree also offers instructor-led training with hands-on experience.[34] While CompTIA recommends 12 months of Linux experience and prior CompTIA A+ and Network+ certifications, these are not strict prerequisites.[16]

Red Hat Certified System Administrator (RHCSA EX200): Enterprise Linux Expertise

The Red Hat Certified System Administrator (RHCSA EX200) is a highly prestigious and performance-based certification from Red Hat, a major player in open-source solutions. This credential validates core system administration skills in Red Hat Enterprise Linux (RHEL) environments.[16] It is also a fundamental prerequisite for the higher-level Red Hat Certified Engineer (RHCE) certification.[16]
The RHCSA exam necessitates practical demonstration of skills, and preparation typically involves two core courses. **Red Hat System Administration I (RH124)** introduces the Linux and RHEL ecosystem, focusing on command-line access, file management, user and group administration with security policies, and the control and monitoring of systemd services. It

also covers configuring remote access using the web console and SSH, managing network interfaces, and software management via DNF. Log analysis, archiving, and transferring files, along with file system access, are also key components.[34] This course includes extensive hands-on labs.[42]

Building upon RH124, **Red Hat System Administration II (RH134)** delves deeper into core Linux administration skills. This includes advanced storage configuration and management using LVM, detailed procedures for installing and deploying Red Hat Enterprise Linux, and the management of critical security features such as SELinux. The course also covers controlling recurring system tasks, managing the boot process, troubleshooting common system issues, basic system tuning, and running containers.[16]

The RHCSA exam is distinctive for its entirely performance-based format, requiring candidates to execute tasks on a live system rather than answering multiple-choice questions.[39] This format is a strong indicator of its real-world applicability and directly addresses the need for certifications that provide verifiable "experience." Unlike theoretical exams, this assessment compels candidates to demonstrate actual competence in a live environment, making the certification highly valuable to employers. This also implies that the learning process for RHCSA

must involve substantial hands-on practice, aligning perfectly with a learning style that thrives on practical application. Both RH124 and RH134 courses incorporate extensive hands-on labs.[41] For example, RH124 labs cover managing files, users, processes, services, configuring SSH, analyzing logs, and managing networking.[41] RH134 labs include improving command-line productivity, scheduling tasks, managing SELinux, logical volumes, network-attached storage, and containers.[47]

Recommended learning resources include **Red Hat Training's official courses (RH124 and RH134)**, which are highly recommended for exam preparation.[38] These courses are available in instructor-led formats (in-person or virtual) and self-paced options.[40] Global Knowledge also offers RHCSA training with hands-on labs.[39] LabEx provides an RH124 course with 14 hands-on labs specifically focused on RHEL system administration essentials.[41] While there are no formal prerequisites for the RHCSA exam, Red Hat strongly recommends completing the RH124 and RH134 courses or possessing equivalent work experience.[38]

Linux Professional Institute (LPI) LPIC-1 (101-500 & 102-500): Foundational Linux Administration

The Linux Professional Institute (LPI) LPIC-1 certification (requiring exams 101-500 and 102-500) offers a foundational, vendor-neutral pathway for demonstrating competence in Linux administration. This certification validates an individual's ability to perform essential maintenance tasks using the command line, install and configure a Linux system, and set up basic networking.[16]

The LPIC-1 curriculum is designed to cover a broad range of fundamental Linux topics. It

includes **System Architecture**, which encompasses hardware settings, the boot process, runlevels, and system shutdown procedures.[52]
Linux Installation and Package Management covers disk partitioning, boot manager configuration, shared libraries, and the use of both Debian and RPM package management systems.[52] The certification delves into
GNU and Unix Commands, focusing on command-line operations, filters, pipes, text processing, and basic shell scripting.[52] It also addresses
Devices, Linux Filesystems, and the Filesystem Hierarchy Standard, including partitions, filesystems, mounting procedures, and managing permissions and ownership.[52]
Shells and Shell Scripting teaches how to customize the shell environment and write simple scripts.[52]
Administrative Tasks cover managing users and groups, scheduling tasks, system logging, and process management.[52]
Essential System Services introduces networking fundamentals, DNS client configuration, and basic web services.[52] Finally,
Security & Networking Fundamentals covers encryption, access control, and network configuration.[52]
The LPIC-1 training by uCertify emphasizes interactive labs and simulated scenarios. Its program includes integrated labs for hands-on experience and simulated real-world scenarios, providing a non-production, risk-free environment for practicing and refining skills.[52] The syllabus incorporates interactive questions at the conclusion of each chapter to help consolidate knowledge, complemented by "Labs and videos to see and do".[52]
Recommended learning resources include the **LPI Official Learning Materials**, which provide detailed exam objectives and learning resources directly on their website.[51]
uCertify offers comprehensive LPIC-1 training specifically designed to aid in passing both exams, featuring interactive items, integrated labs, and practice tests.[52] A notable advantage of LPIC-1 is that it has no formal prerequisites, making it an accessible entry point for individuals new to Linux.[51]

Table 3: Linux/Unix Certifications Comparison

Certification Name	Vendor	Level	Vendor-Neutral/Specific	Key Focus Areas	Exam Format	Hands-on Lab Integration	Typical Learning Resources	Prerequisites
CompTIA Linux+ (XK0-005)	CompTIA	Intermediate	Vendor-Neutral	System management, security,	Multiple-choice & performance-base	CompTIA CertMaster Labs, Dion	Official CompTIA Student Guides/eB	CompTIA A+, Network+, 12 months

				scripting, containers, automation, troubleshooting	d	Training Practice Lab (browser-based virtual labs)	ooks, CertMaster Learn + Labs, ONLC, Learning Tree	Linux experience (recommended)
Red Hat Certified System Administrator (RHCSA EX200)	Red Hat	Intermediate	Vendor-Specific (Red Hat)	RHEL administration, file/user/storage management, security, networking, containers	Performance-based (live system)	Extensive hands-on labs in RH124 & RH134 courses	Red Hat Training (RH124, RH134), Global Knowledge, LabEx	RH124 & RH134 courses or equivalent experience (recommended)
LPIC-1 (101-500 & 102-500)	Linux Professional Institute (LPI)	Foundational	Vendor-Neutral	Command line, installation, configuration, package management, basic networking	Multiple-choice & fill-in-the-blank	Integrated labs and simulated scenarios (e.g., uCertify)	LPI Official Learning Materials, uCertify	None

Ethical Hacking and Penetration Testing: Thinking Like an Attacker

Understanding offensive techniques is paramount for effective defense in cybersecurity. This section directly addresses the interest in "Critical Ethical hacker" by outlining modern certifications that cultivate an attacker's mindset and practical penetration testing skills.

eJPT (eLearnSecurity Junior Penetration Tester): Your First Red Team

Milestone

The eJPT (eLearnSecurity Junior Penetration Tester) certification serves as an excellent entry-level credential, validating the foundational knowledge, skills, and abilities required for a junior penetration tester role.[12] It is specifically designed for individuals with minimal to no prior cybersecurity experience, making it an accessible starting point.[12]
The eJPT certification exam covers several key areas. **Assessment Methodologies** encompass information gathering, footprinting, and scanning techniques.[12]
Host and Network Auditing focuses on identifying open ports and services on a target, determining the operating system, enumerating network, system, and user information, and understanding how to transfer files and gather hash/password data.[12]
Host and Network Penetration Testing delves into identifying and modifying exploit code, performing exploitation with Metasploit, demonstrating pivoting techniques (via routing and port forwarding), and conducting brute-force password attacks and hash cracking.[12] Lastly, **Web Application Penetration Testing** covers identifying vulnerabilities in web applications, locating hidden files and directories, executing brute-force login attacks, and performing web application reconnaissance.[12]
The eJPT certification exam itself is a hands-on, simulated real-world engagement, providing a practical assessment of skills.[12] The
INE Penetration Testing Student Learning Path, which is designed to prepare candidates for the eJPT, includes a substantial number of labs (121 labs).[55] This learning path integrates practical lab time with expert-led courses.[12] The curriculum is structured with modules and hands-on labs that cover essential topics such as passive and active reconnaissance, the use of Nmap, Burp Suite, Metasploit, and various privilege escalation techniques.[53] The design of eJPT as a "first milestone certification for someone with little to no experience" [12] is particularly beneficial. It provides a structured entry point into penetration testing without requiring extensive prior experience, directly addressing the need for foundational prerequisites. The hands-on exam format offers a strong validation of practical skills, ensuring that even beginners gain relevant, verifiable experience, which builds confidence and a foundational skillset for more complex challenges. This makes eJPT an ideal "on-ramp" into the offensive security domain, providing immediate practical application and a clear path forward.
Recommended learning resources include the **INE Penetration Testing Student Learning Path**, which is specifically built for entry-level Red Team professionals and prepares them for the eJPT exam through a blend of expert-led courses and practical lab time.[12] Notably, the labs within this path are often pre-documented as mini write-ups in PDF files, which can be saved and incorporated into personal notes.[55] Additionally,
TryHackMe offers a "Jr Penetration Tester" learning path with 8 modules and 39 hands-on labs, covering pentesting methodologies, enumeration, exploitation, and reporting, serving as a valuable supplement to INE's material.[53] While a basic understanding of cybersecurity

fundamentals is recommended, the eJPT is accessible to individuals with limited prior experience.[12]

CompTIA PenTest+ (PT0-002): Comprehensive Vulnerability Management

CompTIA PenTest+ (PT0-002) is a certification that demonstrates comprehensive knowledge of vulnerability management. It validates an individual's ability to plan and scope penetration testing engagements, including vulnerability scanning, compliance requirements, results analysis, and remediation reporting.[9] This certification focuses on the practical, hands-on aspects of penetration testing.[56]

The curriculum for CompTIA PenTest+ is structured around five core areas. **Planning and Scoping** introduces penetration testing concepts, outlines how to plan and scope engagements, and details the process of gathering background information.[9]

Information Gathering and Vulnerability Scanning covers passive and active reconnaissance techniques, network scanning, enumerating targets, scanning for vulnerabilities, and analyzing basic scripts for exploitation.[56]

Attacks and Exploits delves into exploiting network, wireless, and specialized systems, as well as Windows and Linux vulnerabilities. It also covers web application vulnerabilities, privilege escalation, and post-exploitation techniques such as lateral movement, establishing persistence, and anti-forensics.[9]

Reporting and Communication focuses on analyzing penetration test data, developing recommendations for mitigation strategies, writing and handling reports, and effectively communicating findings to stakeholders.[9] Finally,

Tools and Code Analysis ensures an understanding of industry-standard tools and methodologies used throughout the penetration testing process.[9]

The PenTest+ exam includes both multiple-choice and performance-based scenarios, requiring practical application of skills.[9] Training programs for this certification combine theoretical knowledge with hands-on practice in real-world scenarios.[9] Bootcamps often incorporate real-world penetration testing exercises, covering reconnaissance, exploitation, privilege escalation, and post-exploitation techniques.[57] The structured approach of PenTest+, which covers the entire process of penetration testing from planning to reporting [9], is highly valuable. This comprehensive methodology provides a clear framework for ethical hacking, ensuring that individuals understand the full lifecycle of a penetration test, including legal, ethical, and communication aspects. This prepares them for professional engagements in a corporate environment, making them not just technically proficient but also methodologically sound.

Recommended learning resources include the **Infosec Institute**, which offers comprehensive training that combines theoretical knowledge with hands-on practice.[9]

Training Camp provides a 5-day intensive boot camp featuring CompTIA's proprietary

PenTest+ courseware, study guides, and realistic practice exams, along with real-world penetration testing exercises.[57] Additionally,
e-Careers delivers the course through online training and live labs, covering the official syllabus.[56] While 3-4 years of hands-on information security experience is recommended, it is not a mandatory prerequisite for the PenTest+ exam.[9]

EC-Council Certified Ethical Hacker (CEH v13): Industry-Recognized Hacking Methodology

The EC-Council Certified Ethical Hacker (CEH v13) remains one of the most widely recognized cybersecurity penetration testing certifications. It provides extensive training in adopting an attacker's mindset, incorporating experience with professional-grade hacking tools and over 550 attack techniques.[9] A notable update in CEH v13 is its integration of AI-driven cybersecurity skills, reflecting the evolving threat landscape.[58]
The curriculum is structured across 20 comprehensive learning modules. **Module 01: Introduction to Ethical Hacking** covers information security concepts, attack classification, hacker classes, the CEH Ethical Hacking Framework, Cyber Kill Chain, MITRE ATT&CK, and introduces AI-driven ethical hacking tools, including ChatGPT-powered tools.[58]
Module 02: Footprinting and Reconnaissance delves into advanced Google Hacking Techniques, people search services, dark web footprinting, social networking, Whois, DNS, email footprinting, and AI-powered OSINT tools.[58]
Module 03: Scanning Networks focuses on host, port, service, and OS discovery, as well as scanning techniques that bypass IDS and Firewalls, and AI-powered scanning.[58]
Module 04: Enumeration covers various enumeration types such as NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Unix/Linux user enumeration, and SMB, including AI-driven enumeration techniques.[58]
Module 05: Vulnerability Analysis explores vulnerability classification, scoring systems, databases, research, scanning, assessment tools, and AI-powered analysis.[58]
Further modules cover **System Hacking** (password cracking, exploitation with Metasploit and AI tools, buffer overflow, Active Directory enumeration, privilege escalation, keyloggers, rootkits, steganography, persistence, and covering tracks) [58];
Malware Threats (Trojans, viruses, ransomware, worms, fileless malware, AI-based malware, static/dynamic analysis) [58];
Sniffing (MAC flooding, ARP poisoning, MITM, DHCP starvation, MAC spoofing, VLAN hopping, STP attack, DNS poisoning) [58];
Social Engineering (techniques, phishing detection, AI-powered impersonation) [58];
Denial-of-Service (DoS/DDoS attacks, botnets, detection, protection) [58];
Session Hijacking (application/network level, TCP/IP hijacking, tools, detection) [58]; and
Evading IDS, Firewalls, and Honeypots (evasion techniques, bypassing antivirus).[58] The curriculum also includes

Hacking Web Servers/Applications (reconnaissance, vulnerabilities, attacks like SQL injection and XSS, security testing) [58];
Wireless Networks (footprinting, traffic analysis, WPA2 cracking, rogue APs) [58];
Mobile Platforms, IoT, and OT Hacking (Android/iOS hacking, IoT/OT vulnerabilities/attacks) [58];
Cloud Computing (cloud models, threats, container/Kubernetes vulnerabilities, AWS/Azure/Google Cloud hacking) [58]; and
Cryptography (encryption algorithms, PKI, digital signatures, cryptanalysis, blockchain attacks).[58]
CEH v13 places a strong emphasis on extensive hands-on labs and cyber range practice. It features 221 hands-on labs designed with real-world scenarios and powered by AI.[58] The training provides 100% virtualization, offering full access to pre-configured targets, networks, and attack tools, including vulnerable websites and operating systems, within fully networked environments.[62] A cloud-based cyber range allows for practicing every course objective on live machines.[62] EC-Council provides an OpenAI key for use in the AI labs, and for those unable or unwilling to use OpenAI APIs, a comprehensive Lab Guide with step-by-step instructions and video walk-throughs is available.[62] The integration of AI into CEH v13 is a significant emerging theme, demonstrating EC-Council's commitment to modernizing its curriculum to reflect the evolving threat landscape where AI is increasingly utilized by both attackers and defenders. This forward-thinking approach prepares individuals for future challenges by equipping them with skills relevant to the next generation of cyber threats and defenses, ensuring their knowledge remains current and applicable.
Recommended learning resources include **EC-Council Official Training**, which offers a comprehensive 4-step framework: Learn, Certify, Engage, and Compete. This framework includes knowledge-based training, hands-on labs, cyber range exercises, and Capture The Flag (CTF) challenges.[58] Students receive one-year access to course materials and six months of lab access.[62] The
Infosec Institute, an EC-Council partner, provides approved materials as part of its CEH training.[60] To qualify for the CEH exam, candidates typically need to complete official CEH training or obtain approval through an application process demonstrating relevant experience.[9]

Offensive Security Certified Professional (OSCP PEN-200): The Practical Gold Standard

The Offensive Security Certified Professional (OSCP), associated with the PEN-200: Penetration Testing with Kali Linux course, is a highly coveted and respected ethical hacking certification. It focuses on teaching penetration testing methodologies and the practical use of Kali Linux tools.[10] The OSCP is distinguished by its technical depth and its requirement for demonstrable practical penetration testing skills, validated through a challenging 24-hour

exam.[10]

The PEN-200 course curriculum is designed to be comprehensive and hands-on. It begins with an **Introduction to Cybersecurity**, covering foundational concepts, developing an adversarial mindset, and effective learning strategies.[63] A crucial component is **Report Writing for Penetration Testers**, which teaches the purpose of technical reports, how to tailor content, construct executive summaries, and effectively present technical findings and recommendations.[63]

Information Gathering covers both passive techniques (Open Source Intelligence or OSINT, web server analysis, DNS) and active methods (Netcat, Nmap, DNS, SMB, SMTP, and SNMP enumeration).[63]

Vulnerability Scanning explores how scanners function, different types of scans, and practical aspects like Nessus installation, configuration, and authenticated scans.[63]

Web Application Attacks introduces web applications and common attack vectors, including the use of Burp Suite, API enumeration, Cross-Site Scripting (XSS), Directory Traversal, File Inclusion, and Command Injection, along with SQL Injection techniques.[63]

The course also covers **Client-Side Attacks**, focusing on information gathering and client fingerprinting, and preparing attacks using methods like malicious Microsoft Office documents.[64]

Locating and Fixing Public Exploits teaches how to utilize resources like the Exploit Database, exploit frameworks (SearchSploit, Nmap NSE Scripts), and how to cross-compile and modify existing exploits.[63]

Antivirus Evasion delves into detection methods, in-memory evasion, thread injection, and automating evasion techniques.[63]

Password Attacks covers cracking fundamentals (encryption, hashes), mutating wordlists, cracking methodologies, and attacking password manager key files, SSH private keys, and NTLM.[63]

Privilege Escalation is extensively covered for both Windows (understanding privileges, access control, situational awareness, PowerShell, automated enumeration, service binary/DLL hijacking, unquoted service paths, scheduled tasks) and Linux (manual and automated enumeration, inspecting user trails and service footprints, abusing cron jobs, and password authentication).[63] Additional topics include Port Redirection and Tunneling [65], Active Directory Attacks (including enumeration of OS permissions, Service Principal Names, object permissions, and domain shares) [63], and the use of **The Metasploit Framework** and **PowerShell Empire**.[65]

The OSCP is renowned for its hands-on lab environment and a rigorous 24-hour practical exam. The certification requires individuals to successfully attack and penetrate various live machines within a safe lab environment.[10] The PEN-200 course typically includes 90 days of lab access, with options for 12-month or unlimited access through Learn One/Unlimited subscriptions.[11] These labs are deeply integrated with the course topics, featuring specific exercises for Whois, Google Hacking, Nmap, Burp Suite, SQL Injection, Antivirus Evasion, and various privilege escalation scenarios.[64]

Proving Ground Practice labs are also recommended for additional hands-on experience.[64] The exam itself is a proctored, 24-hour practical test, demanding sustained performance and problem-solving.[11]

The "Try Harder" philosophy espoused by Offensive Security is a unique and profoundly impactful aspect of the OSCP.[63] This philosophy cultivates resilience, critical thinking, and advanced problem-solving skills by pushing learners beyond rote solutions, which is invaluable in a field where novel and unpredictable challenges are constant. This approach extends beyond mere technical instruction, fostering a fundamental shift in mindset. Cybersecurity, especially offensive security, frequently involves encountering unknown, complex, and frustrating problems where memorized solutions are insufficient. The "Try Harder" ethos encourages independent research, creative problem-solving, and perseverance in the face of failure. The structured "learn from failure" approach [66] is a deliberate training method designed to develop grit and adaptability. This means the OSCP's "Try Harder" philosophy trains an individual's
mindset for real-world, unpredictable cybersecurity challenges, making them not only technically proficient but also mentally robust and adaptable, a significant differentiator in the industry.

Recommended learning resources primarily stem from **Offensive Security Official (PEN-200 course)**, which is the authoritative source for OSCP preparation, offering course materials, labs, and exam attempts.[11]

Firebrand Training provides an accelerated boot camp for PEN-200, which includes access to recently retired OSCP exam machines for additional practice.[65] Additionally, a "Free Ebook: OSCP & PEN-200 Prep" from OffSec offers expert tips and deep dives into the PEN-200 experience.[66] Prerequisites for the OSCP include a solid understanding of TCP/IP networking, reasonable Windows and Linux administration experience, and familiarity with basic Bash and/or Python scripting.[11]

Table 4: Ethical Hacking Certifications Comparison

Certification Name	Vendor	Level	Key Focus Areas	Exam Format	Hands-on Lab Integration	Typical Learning Resources	Prerequisites	Estimated Cost (Course + Exam)
eJPT	INE Security	Entry-Level	Assessment methodologies, host/network auditing, pen	Hands-on, simulated engagement	121 labs in PTS Learning Path, exam is hands-on	INE Penetration Testing Student Learning Path, TryHackM	Basic cybersecurity fundamentals (recommended)	~$249 - $299 (Fundamentals Annual) [13]

			testing, web app pen testing			e		
CompTIA PenTest+ (PT0-002)	CompTIA	Intermediate	Pen test planning/scoping, info gathering, attacks, reporting, tools	Multiple-choice & performance-based scenarios	Hands-on practice in real-world scenarios, bootcamps	Infosec Institute, Training Camp, e-Careers	3-4 years info security experience (recommended)	~$392 (exam fee) [9]
EC-Council CEH v13	EC-Council	Intermediate	Ethical hacking methodologies, 550+ attack techniques, AI integration	Knowledge exam (MCQ) + Optional Practical Exam (hands-on)	221 hands-on labs, cloud-based cyber range, AI labs	EC-Council Official Training, Infosec Institute	Official CEH training or relevant experience	~$1199 (exam + proctoring) [9]
Offensive Security OSCP (PEN-200)	Offensive Security	Advanced	Practical pen testing, Kali Linux tools, exploitation, privilege escalation, Active Directory attacks	24-hour performance-based	90+ days lab access, Proving Ground Practice labs	Offensive Security Official (PEN-200 course), Firebrand Training	Solid TCP/IP, Windows/Linux admin, Bash/Python scripting	~$1749 (course + 90 days lab + 1 exam) [11]

Microsoft Cloud Security: Administering Secure Services

The role of a "Microsoft Certified Service Engineer" has significantly evolved, largely

transitioning into cloud administration and security given Microsoft's substantial footprint in cloud computing with Azure. Modern career paths within Microsoft now focus on specialized cloud roles.

Microsoft Certified: Azure Administrator Associate (AZ-104): Cloud Infrastructure Management

The Microsoft Certified: Azure Administrator Associate (AZ-104) is an intermediate-level certification designed for IT professionals who possess foundational Azure knowledge and basic networking skills.[6] This credential equips individuals with the expertise to manage Azure subscriptions, secure identities, administer cloud infrastructure, configure virtual networking, implement storage solutions, and effectively create and scale resources within Azure environments.[5]

The curriculum for AZ-104 is often structured as a three-course series. The first course, **Managing Azure Identity, Governance, and Storage**, covers Azure Active Directory (including users, groups, and licenses), Role-Based Access Control (RBAC), and managing access to Azure subscriptions. It also delves into various storage account types, replication strategies, network access configurations, encryption, Shared Access Signatures (SAS), Blob Storage, and Azure File Sync.[5] The second course, **Azure Storage, Compute, Containers, and Automation**, focuses on configuring Azure storage solutions, automating resource deployments using Azure Resource Manager (ARM) templates and Virtual Machine (VM) extensions. It also covers managing virtual machines, scaling Kubernetes services, and implementing secure Azure App Services.[6] The final course, **Networking, Monitoring, and Backup Strategies**, teaches the design and configuration of Azure Virtual Network peering, VPN Gateway, and hub-and-spoke networks. It covers Load Balancers, Application Gateways, Network Security Groups, DNS, Azure Monitor (for metrics and logs), Azure Backup, and Recovery Services vault configurations.[5]

The specialization includes hands-on projects that accurately simulate real-world scenarios, such as configuring virtual networks, deploying scalable virtual machines, and implementing automated resource deployments.[6] Learning objectives are directly tied to practical implementation, for instance, "Implement network security group rules," "Configure Azure DNS," and "Configure back-end pools".[5] This integrated practical component ensures that theoretical knowledge is immediately applied, reinforcing learning.

Recommended learning resources include **Microsoft Learn**, which provides free, self-paced learning paths specifically aligned with the AZ-104 exam.[4] Coursera offers the **Packt Microsoft Azure Administrator AZ-104 Specialization**, a three-course series that provides hands-on lessons and projects, covering Azure AD management, governance, storage, and networking.[6] Learning Tree also offers Azure Administrator training that encompasses the management of Azure subscriptions, identity, infrastructure, networking, storage, and monitoring.[5] The prerequisites for this intermediate-level certification

recommend foundational Azure knowledge and basic networking skills.[6]

Microsoft Certified: Azure Security Engineer Associate (AZ-500): Specializing in Azure Security

The Microsoft Certified: Azure Security Engineer Associate (AZ-500) certification is tailored for professionals who implement, manage, and monitor security for resources across Azure, multi-cloud, and hybrid environments.[4] This certification is recognized as one of the highest-paying Microsoft Azure certifications, reflecting the high demand for Azure security experts.[7]

The curriculum is meticulously aligned with the AZ-500 exam requirements, covering four key areas. **Secure Identity and Access** focuses on Azure AD Identity Protection, Azure AD Privileged Identity Management (PIM), managing groups and guests, and implementing Azure policies and Role-Based Access Control (RBAC), including multifactor authentication.[4]

Implement Platform Protection delves into defense-in-depth strategies, and the implementation and configuration of Azure Application Gateway and Azure Web Application Firewall (WAF).[4]

Secure Compute, Storage, and Databases covers deploying Shared Access Signatures (SAS), enabling and monitoring database auditing, configuring Microsoft Defender for SQL for advanced threat protection, and deploying Always Encrypted solutions.[4] Finally,

Manage Security Operations focuses on configuring and monitoring metrics and logs in Azure Monitor, managing applications using Azure Monitor Application Insights, implementing and configuring Microsoft Defender for Cloud, and establishing just-in-time VPN access to protect against brute-force attacks, alongside general security posture management and threat protection.[4]

Each course within the Coursera program for AZ-500 integrates theoretical concepts with practice exercises and hands-on exercises in Azure.[7] Scenario-based projects are a core component, allowing for practice in realistic settings. A final comprehensive hands-on project simulates the typical activities of an Azure security engineer, such as implementing multifactor authentication, creating resource groups, and setting up virtual machines with appropriate security groups.[7] The progression from AZ-104 (Azure Administrator) to AZ-500 (Azure Security Engineer) illustrates a logical specialization path within Microsoft Azure. This allows an individual to first acquire foundational cloud management skills and then layer on specific security expertise, a highly sought-after combination in modern IT. This layered approach ensures that the professional understands the underlying infrastructure they are tasked with protecting, enabling them to identify vulnerabilities stemming from misconfigurations and implement more effective security controls. This holistic understanding enhances their value beyond someone with only security knowledge.

Recommended learning resources include **Microsoft Learn**, which provides detailed learning paths for the AZ-500 exam.[4] Coursera offers the

Microsoft Azure Security Engineer Associate Professional Certificate, a seven-course series that combines concepts, practice, and hands-on exercises to prepare for the AZ-500 exam.[7] Global Knowledge also provides live instructor-led training for AZ-500.[8] Prerequisites for this certification include experience in Microsoft Azure and hybrid environments, along with strong familiarity with Microsoft Entra ID, compute, network, and storage in Azure.[4]

Microsoft Certified: Cybersecurity Architect Expert (SC-100): Advanced Security Design

The Microsoft Certified: Cybersecurity Architect Expert (SC-100) is an advanced certification focused on designing, guiding the implementation of, and maintaining security solutions that adhere to Zero Trust principles and best practices. This encompasses security strategies for identity, devices, data, AI, applications, networks, infrastructure, and DevOps.[3] This credential represents the highest level of Microsoft security certification mentioned, marking a shift towards strategic and architectural cybersecurity thinking.

To pursue the SC-100, candidates must first hold at least one of the following associate-level certifications: Microsoft Certified: Azure Security Engineer Associate (AZ-500), Microsoft Certified: Identity and Access Administrator Associate, or Microsoft Certified: Security Operations Analyst Associate.[3] This prerequisite structure clearly defines a progressive learning path. Upon completion, individuals gain skills in designing security operations and compliance capabilities using Microsoft Defender and Microsoft Sentinel, as well as designing application and infrastructure security solutions with these tools.[3] The expertise acquired includes Zero Trust principles, Governance Risk Compliance (GRC), security operations (SecOps), data and application security, and experience with hybrid and multi-cloud implementations.[3]

The SC-100's emphasis on "designing, guiding the implementation of, and maintaining security solutions that follow Zero Trust principles" [3] highlights a critical evolution in modern enterprise security. This focus signifies a move from traditional perimeter-based defense to a "never trust, always verify" model. This paradigm shift acknowledges that threats can originate from anywhere, both internal and external to an organization's network. Designing security solutions based on Zero Trust requires a deep understanding of entire IT ecosystems, rather than just individual components. This advanced perspective positions an individual to transition from an operational role (e.g., administrator, engineer) to a strategic, leadership position. This prepares the professional for senior-level roles where they influence the overall security posture and architecture of an organization, directly addressing the "architect" aspect of the initially outdated query.

Recommended learning resources for SC-100 are primarily found on **Microsoft Learn**, which provides modules for the exam. These modules concentrate on designing solutions that align with security best practices, operations, identity, compliance, application, data, and infrastructure security.[3]

Table 5: Microsoft Cloud Security Certifications Progression

Certification Name	Level	Key Focus	Prerequisites	Skills Gained	Typical Job Roles
Microsoft Certified: Azure Administrator Associate (AZ-104)	Intermediate	Azure infrastructure management, identity, networking, storage, compute, automation	Foundational Azure knowledge, basic networking	Manage Azure AD, virtual networks, storage, VMs, backup/recovery	Azure Administrator, Cloud Administrator, IT Systems Manager
Microsoft Certified: Azure Security Engineer Associate (AZ-500)	Intermediate	Implementing, managing, and monitoring security in Azure, multi-cloud, hybrid environments	Experience in Azure environments, familiarity with Azure AD, compute, network, storage	Secure identity/access, platform protection, data/apps, manage security operations	Azure Security Engineer, Security Analyst, Cloud Security Engineer
Microsoft Certified: Cybersecurity Architect Expert (SC-100)	Expert	Designing and guiding implementation of Zero Trust security solutions across entire enterprise	AZ-500 OR Identity and Access Administrator Associate OR Security Operations Analyst Associate	Design SecOps, compliance, application, infrastructure security solutions	Cybersecurity Architect, Enterprise Security Architect, Security Consultant

Integrated Learning Path and Next Steps

A Suggested Progression for Your Cybersecurity Career

To effectively navigate the modern cybersecurity landscape, a layered learning approach is highly recommended, building from broad foundational IT knowledge to specialized security

domains. This mirrors the real-world complexity of cybersecurity, where effective defense requires understanding both the underlying systems and the specific attack vectors.

Phase 1: Foundational IT & Networking (0-6 months)

Begin by establishing a robust understanding of core IT and networking principles.

- **CompTIA A+ (Optional but Recommended)**: This certification provides a broad understanding of IT fundamentals, covering hardware, software, and troubleshooting, which serves as an excellent general IT baseline.
- **CompTIA Network+ (N10-009)**: This is essential for understanding how networks operate and how to secure them. It offers vendor-neutral knowledge that is universally applicable across different hardware and software vendors, providing a broad base before any specialization.
- **Cisco CCNA (200-301) (Alternative/Complement to Network+)**: For a deeper dive into Cisco networking, which is highly valued in the industry, the CCNA is an excellent choice. The use of Cisco Packet Tracer and Network Simulator Lite allows for experimentation with complex network configurations in a risk-free, virtual environment, bridging the gap between theoretical knowledge and practical application without requiring expensive physical equipment. This democratizes practical networking education, making it accessible and repeatable for solidifying understanding.
- **Linux Fundamentals (Concurrent)**: Concurrently, begin building core Linux administration skills. The **CompTIA Linux+** or **LPI LPIC-1** certifications are excellent starting points, as Linux is pervasive in cybersecurity tools, servers, and cloud environments.

Phase 2: Core Cybersecurity & Linux Mastery (6-18 months)

Once foundational IT and networking skills are established, transition into core cybersecurity concepts and deepen Linux expertise.

- **CompTIA Security+ (SY0-701)**: This is a critical foundational security certification that covers broad security concepts, threats, and controls. It is often a prerequisite for entry-level security roles and provides a vendor-neutral understanding of cybersecurity principles.
- **Deep Dive into Linux (Concurrent)**: Progress to **Red Hat RHCSA** for enterprise-level Linux administration, especially if aiming for roles involving Red Hat environments. The performance-based nature of the RHCSA exam is a strong indicator of its real-world applicability, as it requires candidates to perform tasks on a live system, providing undeniable proof of hands-on ability. This translates directly into confidence for employers that the candidate can perform the job.
- **Introduction to Ethical Hacking (Concurrent)**: Begin with **eJPT** for hands-on, entry-level penetration testing skills. The eJPT's design as a "first milestone certification for someone with little to no experience" makes it a crucial structured entry point into offensive security, providing immediate practical application and a clear path forward for those without extensive prior experience.

Phase 3: Specialization & Advanced Skills (18+ months)

This phase involves specializing in specific cybersecurity domains based on career interests.

- **Ethical Hacking Specialization**: Choose between **CompTIA PenTest+** (which offers a

comprehensive, process-oriented approach to penetration testing, including planning and reporting) or **EC-Council CEH** (which provides a broad understanding of hacking tools and techniques, now integrated with AI). For the most practical and challenging path, pursue **Offensive Security OSCP**. The "Try Harder" philosophy of Offensive Security cultivates resilience, critical thinking, and problem-solving skills by pushing learners beyond rote solutions, which is invaluable for a field where novel challenges are constant.

- **Cloud Security Specialization**: Begin with **Microsoft Certified: Azure Administrator Associate (AZ-104)** to understand cloud infrastructure management. Then, advance to **Microsoft Certified: Azure Security Engineer Associate (AZ-500)** for dedicated cloud security roles. This layered certification approach ensures a robust and practical skillset, allowing individuals to understand *what* they are securing and *how* it operates, which is critical for effective cloud cybersecurity.
- **Advanced Architecture (Long-term Goal)**: For those aspiring to design and strategic security roles, the **Microsoft Certified: Cybersecurity Architect Expert (SC-100)** is the ultimate goal. Its focus on "Zero Trust principles" highlights a critical shift in modern enterprise security, positioning individuals for senior-level roles where they influence the overall security posture of an organization.

This phased approach ensures a solid knowledge base, preventing "skill silos" and allowing for the development of a holistic understanding of cybersecurity, making individuals more adaptable and effective in diverse roles.

Leveraging Certifications for Job Opportunities

Certifications such as CompTIA Security+, Cisco CCNA, Microsoft AZ-500, and Offensive Security OSCP are highly recognized credentials that can significantly enhance job prospects and earning potential in the cybersecurity market.[7] The inclusion of extensive hands-on labs and performance-based exams in these certifications provides tangible proof of skills, which is highly valued by employers. This practical validation assures employers that candidates possess verified, up-to-date competencies, thereby reducing hiring risk and streamlining talent acquisition.[10] The frequent correlation between certifications and specific job roles and salary potential underscores that these credentials are not merely academic achievements but direct pathways to career advancement and increased earning potential in a high-demand field. These certifications serve as a crucial currency in the cybersecurity job market, translating directly into enhanced employability and financial benefits, making the investment in them a strategic career move.

Beyond formal training, engaging with learning platforms and professional communities can lead to valuable networking opportunities and job support.[2]

The Importance of Continuous Learning and Community Engagement

Cybersecurity is an inherently dynamic field, with threats, technologies, and attack techniques constantly evolving. This necessitates a commitment to continuous learning to remain effective and current.[11] Many certifications, such as those from CompTIA, EC-Council, LPI, and Offensive Security, have validity periods (typically 3-5 years) that require renewal or the attainment of higher-level certifications.[9] This built-in obsolescence of certifications, requiring renewal, is a deliberate feature. It reflects the critical need for perpetual skill development in cybersecurity, ensuring that professionals remain current and competent in a rapidly changing threat landscape. This prepares individuals for a career path that demands continuous adaptation and learning, a key characteristic of success in this domain.
Furthermore, active participation in professional communities and forums, often facilitated by learning platforms, fosters an environment for sharing problems, finding solutions, and refining skills.[14] This collaborative aspect is vital for staying informed about emerging threats and best practices.

Table 6: Course Content & Lab Integration Summary (per certification)

Certification Name	Key Curriculum Areas (Modules/Chapters)	Lab Type & Integration	Written Material Format	Chapter-by-Chapter Application Support
CompTIA Network+ (N10-009)	Networking Concepts, Infrastructure, Network Operations, Network Security, Troubleshooting	Integrated labs, simulated real-world scenarios (uCertify); Virtual labs (CertMaster Labs)	Official Study Guides, eBooks, Digital Courseware	Yes, with interactive questions after chapters [14]
Cisco CCNA (200-301)	Network Fundamentals, IP Connectivity, IP Services, Security Fundamentals, Automation	Cisco Packet Tracer, Network Simulator Lite (34 free labs), interactive labs	Official Cert Guides (PDF/eBook), Digital Courseware	Yes, with practice labs and quizzes per module [1]
CompTIA Linux+ (XK0-005)	System Management, Security, Scripting/Containers/Automation, Troubleshooting	CertMaster Labs (browser-based virtual labs), Dion Training Practice Lab (simulated)	Official Student Guides/eBooks, Digital Courseware	Yes, extensive step-by-step activities aligned with objectives [17]

Red Hat Certified System Administrator (RHCSA EX200)	System Administration I (RH124) & II (RH134) topics: file/user/group mgmt, networking, security, storage, scripting, containers	Extensive hands-on labs in RH124/RH134 courses, performance-based exam on live system	Student Workbooks (PDF), Official Training Curriculum	Yes, task-focused activities and lab-based knowledge checks [41]
LPIC-1 (101-500 & 102-500)	System Architecture, Installation/Package Management, GNU/Unix Commands, Filesystems, Shell Scripting, Admin Tasks, Services, Security/Networking Fundamentals	Integrated labs, simulated real-world scenarios (uCertify)	Official Study Guide, Digital Courseware, Flashcards	Yes, interactive questions at end of chapters, labs/videos [52]
eJPT (eLearnSecurity Junior Penetration Tester)	Assessment Methodologies, Host/Network Auditing, Host/Network Pen Testing, Web App Pen Testing	Hands-on exam, 121 labs in PTS Learning Path, simulated engagements	Expert-led courses, PDF write-ups for labs, notes from community	Yes, blend of expert-led courses and practical lab time [12]
CompTIA PenTest+ (PT0-002)	Planning/Scoping, Info Gathering/Scanning, Attacks/Exploits, Reporting/Communication, Tools/Code Analysis	Performance-based scenarios in exam, real-world pen test exercises in bootcamps	Proprietary Courseware, Study Guides, Practice Exams	Yes, comprehensive syllabus with practical exercises [9]
EC-Council CEH v13	20 modules covering hacking phases, attack techniques, AI integration, web/mobile/IoT/cl	221 hands-on labs, cloud-based cyber range, AI-powered labs	Official Course Materials, Cheat Sheets, Lab Guides (with screenshots/videos)	Yes, knowledge-based training and hands-on labs with real-world scenarios [58]

	oud hacking			
Offensive Security OSCP (PEN-200)	Intro to Cybersecurity, Report Writing, Info Gathering, Vulnerability Scanning, Web App Attacks, Exploits, AV Evasion, Password Attacks, Privilege Escalation, AD Attacks	24-hour practical exam, 90+ days lab access, Proving Grounds Practice labs	Learning Modules, Free Ebook (OSCP & PEN-200 Prep), OffSec Academy Recordings	Yes, week-by-week learning plan with topic labs, capstone labs, challenge labs [11]
Microsoft Certified: Azure Administrator Associate (AZ-104)	Identity/Governance/Storage, Storage/Compute/Containers/Automation, Networking/Monitoring/Backup	Hands-on projects simulating real-world scenarios	Official Microsoft Learn paths, Course Instructor materials, Digital Courseware	Yes, hands-on lessons ensure practical application of concepts [5]
Microsoft Certified: Azure Security Engineer Associate (AZ-500)	Secure Identity/Access, Platform Protection, Compute/Storage/Databases, Security Operations	Scenario-based projects, comprehensive hands-on project	Official Microsoft Learn paths, Course Instructor materials, Digital Courseware	Yes, concepts, practice exercises, and hands-on exercises in Azure [4]
Microsoft Certified: Cybersecurity Architect Expert (SC-100)	Design security solutions (Zero Trust, GRC, SecOps, identity, devices, data, AI, apps, network, infra, DevOps)	Focus on design and strategy, likely architectural labs/case studies	Official Microsoft Learn modules	Yes, modules focus on designing solutions aligning with best practices [3]

Conclusions & Recommendations

The journey into cybersecurity, particularly when transitioning from older paradigms, requires

a strategic and adaptable approach. The analysis confirms that the industry has decisively moved away from broad, generalist certifications towards specialized, hands-on, and cloud-integrated credentials. This shift underscores a fundamental demand for professionals who can demonstrate practical competence in specific domains, rather than merely possessing theoretical knowledge.

For individuals seeking to enter cybersecurity, the following actionable recommendations are provided:

1. **Establish Foundational Pillars**: Prioritize building a strong foundation in both networking and operating systems.
    - **Networking**: Begin with **CompTIA Network+** for its vendor-neutral, universally applicable knowledge of network operations and security. This provides a broad conceptual framework. Complement this with **Cisco CCNA** for a deeper, industry-standard understanding of network devices and configurations. The virtual lab environments provided by these certifications are invaluable for practical, risk-free learning.
    - **Operating Systems**: Concurrently, immerse in Linux/Unix. **CompTIA Linux+** offers a vendor-neutral pathway to core administration skills, including modern aspects like scripting and containers. For enterprise-level proficiency, pursue the **Red Hat Certified System Administrator (RHCSA)**. The performance-based nature of the RHCSA exam is a robust validation of practical skills, directly aligning with the need for demonstrable experience. The **LPI LPIC-1** provides an excellent entry point for those new to Linux, with a focus on command-line mastery and basic administration.
2. **Embrace Practical Ethical Hacking**: Develop an offensive security mindset to understand and counter threats effectively.
    - **Entry-Level Offensive Security**: Start with **eJPT** as a first milestone. Its hands-on exam and integrated labs within the INE Penetration Testing Student Learning Path provide immediate, practical experience for aspiring junior penetration testers, even with limited prior cybersecurity experience.
    - **Structured Penetration Testing**: Progress to **CompTIA PenTest+** to gain a comprehensive understanding of the entire penetration testing lifecycle, from planning and scoping to execution and reporting. This certification emphasizes the professional methodology required for ethical engagements.
    - **Advanced Practical Exploitation**: For a deep dive into hands-on exploitation and Kali Linux tools, the **Offensive Security Certified Professional (OSCP)** is highly recommended. The "Try Harder" philosophy embedded in the OSCP training cultivates critical thinking and resilience, essential traits for navigating complex and unpredictable cybersecurity challenges.
    - **Broad Hacking Techniques**: Consider **EC-Council CEH v13** for its wide array of attack techniques and its integration of AI-driven tools, which prepares professionals for the evolving threat landscape.
3. **Specialize in Cloud Security**: Given the pervasive nature of cloud environments, acquiring cloud-specific security skills is crucial.

    - **Cloud Administration**: Begin with **Microsoft Certified: Azure Administrator Associate (AZ-104)** to build foundational knowledge in managing Azure infrastructure. This understanding is crucial for securing cloud resources effectively.
    - **Cloud Security Engineering**: Advance to **Microsoft Certified: Azure Security Engineer Associate (AZ-500)** to specialize in implementing, managing, and monitoring security within Azure environments. This layered approach ensures a holistic understanding of both cloud administration and security.
    - **Security Architecture**: For those aspiring to strategic design roles, the **Microsoft Certified: Cybersecurity Architect Expert (SC-100)**, with its focus on Zero Trust principles, positions individuals to influence an organization's overall security posture.
4. **Commit to Continuous Learning**: Cybersecurity is a dynamic field where knowledge quickly becomes outdated.
    - **Recertification**: Most modern certifications have validity periods, necessitating renewal or progression to higher-level credentials. This ensures skills remain current and relevant to the evolving threat landscape.
    - **Community Engagement**: Actively participate in professional communities and forums. Sharing knowledge and collaborating with peers is vital for staying informed about emerging threats, tools, and best practices.

By following this structured and practical roadmap, individuals can acquire the necessary skills, knowledge, and experience to successfully enter and advance within the modern cybersecurity domain, aligning their capabilities with current industry demands and future challenges.

Works cited

1. CCNA: Introduction to Networks - Cisco Networking Academy, accessed June 26, 2025, https://www.netacad.com/courses/ccna-introduction-networks
2. Cisco CCNP Security Core Training Online (SCOR 350-701) - PyNet Labs, accessed June 26, 2025, https://www.pynetlabs.com/ccnp-security-core-scor-training/
3. Microsoft Certified: Cybersecurity Architect Expert - Certifications, accessed June 26, 2025, https://learn.microsoft.com/en-us/credentials/certifications/cybersecurity-architect-expert/
4. Microsoft Certified: Azure Security Engineer Associate - Certifications, accessed June 26, 2025, https://learn.microsoft.com/en-us/credentials/certifications/azure-security-engineer/
5. Microsoft Azure Administrator Training (AZ-104) - Learning Tree, accessed June 26, 2025, https://www.learningtree.com/courses/microsoft-azure-administration-training/
6. Microsoft Azure Administrator (AZ-104) | Coursera, accessed June 26, 2025,

https://www.coursera.org/specializations/packt-mircrosoft-azure-administrator-az-104
7. Microsoft Azure Security Engineer Associate (AZ-500) Professional ..., accessed June 26, 2025, https://www.coursera.org/professional-certificates/microsoft-azure-security-engineer-associate
8. Microsoft Azure Security Technologies (AZ-500) - Global Knowledge, accessed June 26, 2025, https://www.globalknowledge.com/us-en/course/178207/microsoft-azure-security-technologies-az-500/
9. Top 10 Penetration Testing Certifications for 2025 - Infosec, accessed June 26, 2025, https://www.infosecinstitute.com/resources/professional-development/top-5-penetration-testing-certifications-security-professionals/
10. Offensive Security Certified Professional - Wikipedia, accessed June 26, 2025, https://en.wikipedia.org/wiki/Offensive_Security_Certified_Professional
11. What Is OSCP Certification and Is It Worth It? 2025 Guide - Coursera, accessed June 26, 2025, https://www.coursera.org/articles/oscp
12. eJPT Certification – INE Security, accessed June 26, 2025, https://security.ine.com/certifications/ejpt-certification/
13. Junior Penetration Tester (eJPT) Certification - INE, accessed June 26, 2025, https://info.ine.com/ejpt/
14. Join Online Computer Courses & Hands-On Labs | uCertify, accessed June 26, 2025, https://www.ucertify.com/p/comptia-network-certification.html
15. CompTIA Network+ Course - New Horizons, accessed June 26, 2025, https://www.newhorizons.com/course-outline/courseid/200001083/coursename/comptia-network-plus
16. The Best Linux Certifications for 2024 - CompTIA, accessed June 26, 2025, https://www.comptia.org/en-us/blog/best-certifications-for-linux/
17. CertMaster Labs for CompTIA Linux + Training | CompTIA IT ..., accessed June 26, 2025, https://www.comptia.org/training/certmaster-labs/linux
18. Cisco Certified Network Associate (CCNA) Training | Learn CCNA Online - Udemy, accessed June 26, 2025, https://www.udemy.com/topic/cisco-ccna/
19. CCNA: Switching, Routing, and Wireless Essentials, accessed June 26, 2025, https://www.netacad.com/courses/ccna-switching-routing-wireless-essentials
20. CCNA: Switching, Routing, and Wireless Essentials - Cisco Networking Academy, accessed June 26, 2025, https://www.netacad.com/fr/courses/ccna-switching-routing-wireless-essentials
21. CCNA: Enterprise Networking, Security, and Automation, accessed June 26, 2025, https://www.netacad.com/courses/ccna-enterprise-networking-security-automation
22. CCNA3v7: Enterprise Networking, Security, and Automation, accessed June 26, 2025, https://account.scte.org/education/course-offerings/course-catalog/ccna3v7-enterprise-networking-security-and-automation-2/

23. CCNA: Introduction to Networks - Cisco Networking Academy, accessed June 26, 2025, https://prelogin-authoring.netacad.com/courses/networking/ccna-introduction-networks
24. CCNA 200-301: Official Cert Guide, Volume 1 - elhacker.INFO, accessed June 26, 2025, https://elhacker.info/manuales/Redes/CCNA-200-301%201.pdf
25. CCNA 200-301 Official Cert Guide Library, 2nd Edition | Cisco Press, accessed June 26, 2025, https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-library-9780138221393
26. CCNA 200-301 Official Cert Guide, Volume 1 - Cisco Press, accessed June 26, 2025, https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-1-9780135792735
27. CCNA 200-301 Official Cert Guide Library[Book] - O'Reilly Media, accessed June 26, 2025, https://www.oreilly.com/library/view/ccna-200-301-official/9780136755562/
28. Cisco Ccna 200-301 Study Guide, 2024 | PDF - Scribd, accessed June 26, 2025, https://www.scribd.com/document/757642397/Cisco-Ccna-200-301-Study-Guide-2024
29. CCNA 200-301 Official Cert Guide, Volume 1, Second Edition, accessed June 26, 2025, https://faspco.com/academy/Ebook/Cisco/CCNA%20200-301%20Official%20Cert%20Guide%20Volume%201%20Second%20Edition.pdf
30. CompTIA Linux+ Certification Training Course Outline | ONLC, accessed June 26, 2025, https://www.onlc.com/outline.asp?ccode=xlxk05
31. The New CompTIA Linux+: Your Questions Answered, accessed June 26, 2025, https://www.comptia.org/en-us/blog/the-new-comptia-linux-your-questions-answered/
32. CompTIA Linux+ XK0-005, accessed June 26, 2025, https://nsu.theknowledgebase.org/connect-anytime-online/catalog/course-description/comptia-linux+-xk0-005/2995/137
33. CompTIA Linux+ Certification (XK0-005) from VTEC Training Education Center | NICCS, accessed June 26, 2025, https://niccs.cisa.gov/education-training/catalog/vtec-training-education-center/comptia-linux-certification-xk0-005
34. CompTIA Linux+® Certification Training - Learning Tree, accessed June 26, 2025, https://www.learningtree.com/courses/comptia-linux-plus-certification-training/
35. CompTIA Integrated CertMaster Learn + Labs for Linux+ (XK0-005), accessed June 26, 2025, https://learnexcelgrow.org/product/comptia-integrated-certmaster-learn-labs-for-linux-xk0-005/
36. Search results for linux+ - CompTIA Marketplace Academic, accessed June 26, 2025, https://academic-store.comptia.org/search?query=linux%2B&categoryId=11352

37. CompTIA Linux+ (XK0-005) Lab - Dion Training Solutions, accessed June 26, 2025, https://www.diontraining.com/products/comptia-linux_lab-001
38. What Is the RHCSA (Red Hat Certified System Administrator) Certification? - Coursera, accessed June 26, 2025, https://www.coursera.org/articles/rhcsa
39. RHCSA – Red Hat Certified System Administrator - Global Knowledge, accessed June 26, 2025, https://www.globalknowledge.com/us-en/training/certification-prep/brands/red-hat/section/red-hat-certifications/rhcsa-red-hat-certified-system-administrator/
40. Red Hat System Administration I | RH124, accessed June 26, 2025, https://www.redhat.com/en/services/training/rh124-red-hat-system-administration-i
41. Red Hat System Administration (RH124) Certification Labs | RHCSA Foundation - LabEx, accessed June 26, 2025, https://labex.io/courses/red-hat-system-administration-rh124-labs
42. Red Hat System Administration I (RH124) Training - Learning Tree, accessed June 26, 2025, https://www.learningtree.com/courses/red-hat-system-administration-i-rh124/
43. RH124 - Red Hat System Administration I - Lumify Work, accessed June 26, 2025, https://www.lumifywork.com/en-au/courses/rh124-red-hat-system-administration-i/
44. RH124 Red Hat System Administration I - QA, accessed June 26, 2025, https://www.qa.com/en-us/course-catalogue/courses/rh124-red-hat-system-administration-i-rh124/
45. Red Hat System Administration I - lectures and labs - Insight, accessed June 26, 2025, https://www.insight.com/en_US/shop/product/RH124/red%20hat%20software/RH124/Red-Hat-System-Administration-I-lectures-and-labs/
46. Red Hat Enterprise Linux Administration 9.0 RH134 pdf - SlideShare, accessed June 26, 2025, https://www.slideshare.net/slideshow/red-hat-enterprise-linux-administration-9-0-rh134-pdf/270217663
47. Red Hat System Administration II (RH134) - New Horizons, accessed June 26, 2025, https://www.newhorizons.com/course-outline/courseid/200007011/coursename/red-hat-system-administration-ii-rh134
48. Red Hat System Administration II Training - LearnQuest, accessed June 26, 2025, https://www.learnquest.com/course-detail-v3.aspx?cnum=RHT-RH134
49. Red Hat System Administration II (RH134) – RHEL 9 Training - Koenig-solutions.com, accessed June 26, 2025, https://www.koenig-solutions.com/red-hat-system-administration-ii-rh134-rhel8-training-course
50. Red Hat System Administration II | RH134, accessed June 26, 2025, https://www.redhat.com/en/services/training/rh134-red-hat-system-administration-ii
51. Our Certifications - Linux Professional Institute (LPI), accessed June 26, 2025,

https://www.lpi.org/our-certifications/summary-of-lpi-certifications/
52. Join Online Computer Courses & Hands-On Labs | uCertify, accessed June 26, 2025, https://www.ucertify.com/p/lpic-1-linux-administrator-certification.html
53. Jr Penetration Tester Training - TryHackMe, accessed June 26, 2025, https://tryhackme.com/path/outline/jrpenetrationtester
54. nyxragon/ejpt-roadmap: This repository contains a roadmap for preparing for the EJPTv2 exam. - GitHub, accessed June 26, 2025, https://github.com/nyxragon/ejpt-roadmap
55. How I Passed eJPT v2 in Just 30 Days! | by Samithran Ramesh - Medium, accessed June 26, 2025, https://medium.com/@samithranramesh/ejpt-v2-the-best-beginner-penetration-testing-certificate-4252f0822002
56. Official CompTIA PenTest+ (PT0-002 Cyber Security Series) Certification - e-Careers, accessed June 26, 2025, https://www.e-careers.com/courses/official-comptia-pentest-pt0-002-cyber-security-series-certification
57. CompTIA PenTest+ Boot Camp - Courses - Training Camp, accessed June 26, 2025, https://trainingcamp.com/training/comptia-pentest-plus-certification-bootcamp/
58. CEH Certification | Ethical Hacking Training & Course - EC-Council, accessed June 26, 2025, https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/
59. Certified Ethical Hacker (CEH) from EC-Council - NICCS - CISA, accessed June 26, 2025, https://niccs.cisa.gov/training/catalog/eccouncil/certified-ethical-hacker-ceh
60. Certified Ethical Hacker (CEH) certification hub - Infosec, accessed June 26, 2025, https://www.infosecinstitute.com/training/ceh/
61. CEH v13 Exam Guide 2025: What You Need to Know? - Axximum Infosolutions, accessed June 26, 2025, https://www.axximuminfosolutions.com/article/ceh-v13-exam-guide-2025/
62. CEH Certification | Ethical Hacking Training & Course | EC-Council, accessed June 26, 2025, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
63. Offsec PEN-200 Course - OSCP Certification - QA, accessed June 26, 2025, https://www.qa.com/course-catalogue/courses/offsec-pen-200-oscp-qaofsecoscp/
64. OffSec PEN-200 Learning Plan - 12 Week, accessed June 26, 2025, https://help.offsec.com/hc/en-us/articles/15541765522196-OffSec-PEN-200-Learning-Plan-12-Week
65. Offensive Security PEN-200: Penetration Testing with Kali Linux | Accelerated course, accessed June 26, 2025, https://firebrand.training/uk/courses/offensive-security/pen-200-penetration-testing-with-kali-linux-certification
66. Free Ebook: OSCP & PEN-200 Prep - OffSec, accessed June 26, 2025, https://www.offsec.com/resources/guides/ebook-oscp-prep-pen200/
67. 8 Popular Cybersecurity Certifications [2025 Updated] - Coursera, accessed

June 26, 2025,
https://www.coursera.org/articles/popular-cybersecurity-certifications