Hewlett Packard Enterprise

HPE Digital Learner Certified Ethical Hacker Content Pack

HPE Content Pack number	CP036
Content Pack length	38 Hours
Content Pack category	Category 2
Learn more	**View now**

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

This course provides learners with the knowledge and abilities to assess the security of computer systems. Students learn how to look for weaknesses and vulnerabilities in target systems using the same knowledge and tools used by malicious hackers (but in a lawful and legitimate manner in order to make the assessment).

Audience

This course significantly benefits security officers, auditors, security

professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure, or is interested in Certified Ethical Hacker credentials.

Objectives

The objective of this course is to prepare professional information security specialists for credentialing in ethical hacking. The goal is have individuals meet or exceed the minimum prescribed standards of the Certified Ethical Hacker.

Examination

- Exam Reference: 312-50 (Certified Ethical Hacker)
- Number of questions: 125
- Types of questions: Multiple choice
- Time allowed to complete: 4 hours
- Recommended level of experience: At least 2 years of relevant security-related experience
- Passing score: 70% (or 88 correct questions)

Next Steps

There are a number of pathways to take following your Ethical Hacker certification. We suggest you look at the other CompTIA courses available within the HPE Digital Learner.

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Detailed Content Pack outline

CEHv10: Ethical Hacking Overview and Threats	• Describe the purpose and knowledge requirements of CEHv10 exam • Describe threats, the general threat landscape, basic terms, and common IT security objectives	• Describe motivations common to the threat actor and define threat categories, attack vectors, and types of defenses against threats
CEHv10: Hacking Concepts	• Define hacking and describe hacking concepts	• Describe hacking phases, such as recon, scanning, access, maintaining access, and covering tracks
CEHv10: Security Controls	• Describe key security controls like information assurance, information security, network segmentation, defense-in-depth, and security policies • Include workplace policies, SecPol creation steps, HR, and legal to begin the process to develop basic security policies	• Describe physical security policies and explore risk management and threat modeling
CEHv10: Security Controls Part 2	• Develop an incident management and response procedure and describe SIEM and UBA	• Describe access controls, the different types of access control mechanisms, data leakage, leak prevention, and data loss prevention
CEHv10: Pentesting, Laws, and Standards	• Describe the types, phases, and methodologies of penetration testing, and how it helps with security assessments	• Recognize common security laws, regulations and standards created by industries and government bodies
CEHv10: Footprinting	• Use footprinting techniques to passively collect info from a target website • Use footprinting and web-based tools to gather information on a target website	• Use whois, traceroute, recon-ng, and other tools to collect info on a target website
CEHv10: Host Discovery and Scanning with Nmap	• Describe how to discover hosts and use common system tools like ping, Nmap, and scripting to perform host discovery • Use Nmap host scanning techniques to perform stealth, TCP connect, ACK, XMAS, and other scans to find hosts, including hosts that may be hidden	• Use Nmap to target specific hosts and gain info on the operating system, open ports, and active services by performing port, UDP, and TCP scans
CEHv10: ProxyChains and Enumeration	• Use ProxyChains to bypass security features like IDS and firewalls to access a target network or segregated internal network	• Perform enumeration and describe the types of things commonly targeted during enumeration
CEHv10: Vulnerability Analysis Concepts and Tools	• Describe the Vulnerability Management Life-Cycle and perform a vulnerability assessment	• Use vulnerability tools like Nikto and MBSA and use references like CVSS and NVD
CEHv10: Password Attacks	• Describe how attacks against passwords can be done with both low and high tech approaches	• Use tools like Medusa and Hydra to attack online passwords and packet sniffing tools like Wireshark to intercept passwords passing through a network
CEHv10: Password Attacks Part 2	• Use popular password cracking tools like John the Ripper and Hashcat to crack passwords • Use GUI based password cracking tools like Ophcrack and gather password hashes for later cracking	• Use man-in-the-middle attacks and pass-the-hash to gain access without cracking the password hash

CEHv10: Privilege Escalation	• Use DLL hijacking and file/folder permission exploitation to gain higher privileges • Use scheduled tasks and insecure sudo implementations to gain higher privileges	• Use operating system vulnerabilities, webshells, and other techniques to gain unauthorized privileges
CEHv10: Covert Data Gathering	• Describe how spyware and keyloggers can be used to capture keystrokes, screenshots, and even audio/video data	
CEHv10: Hidden Files and Covering Tracks	• Describe why hiding files is necessary and show the use of alternate data streams and steganography as tactics for hiding information	• Describe the concept of covering your tracks after you've breached a system, including how to remove traces of your activities by disabling auditing systems and clearing logs
CEHv10: Malware Threats	• Describe malware threats that can be used to attack a system	
CEHv10: Malware Distribution	• Describe how malware is distributed and the components involved	
CEHv10: Network Sniffing	• Describe the purpose behind networking sniffing and use Wireshark to sniff network traffic	• Use MAC flooding, port stealing, and ARP poisoning to sniff packets on a switched network
CEHv10: Denial of Service	• Describe the types of DoS/DDoS attacks, differences between them, and the concepts behind amplification and reflective DoS attacks • Describe volumetric attacks like the Ping of Death, Smurf, Fraggle, UDP flood, and ICMP flood attacks	• Describe protocol type attacks, application layer attacks like HTTP GET/POST and Slowloris using Metasploit, and DoS tools like the High and Low Orbit Ion Cannons
CEHv10: Session Hijacking	• Describe the possible impact of a successful session hijacking attack, conduct a session replay attack by sniffing session tokens, and deploy a cross-site scripting (XSS) attack • Describe token prediction, Cross-Site Request Forgery (CSRF/XSRF), session fixation, and Man-in-the-Browser attacks	• Demonstrate network-layer session hijacking and describe the possible mitigation strategies
CEHv10: Evading IDS, Firewalls, and Honeypots	• Describe IDS, firewalls, and honeypots and use Nmap to evade firewalls	• Describe a honeypot setup and scan against it to potentially see inbound traffic
CEHv10: Evading IDS, Firewalls, and Honeypots Part 2	• Install Snort intrusion detection software	• Configure Snort post-installation and describe the structure of a ruleset
CEHv10: Evading IDS, Firewalls, and Honeypots Part 3	• Test your Snort configuration	
CEHv10: Hacking Web Servers	• Describe common attack tactics, techniques used when hacking web servers, possible motivations for targeting web servers, vulnerabilities associated with web servers, and the common methodologies employed	
CEHv10: Common Web App Threats	• Describe threats against web apps and injection-based attacks	• Use file and directory attacks to lead to unauthorized remote access and code execution
CEHv10: Common Web App Threats Part 2	• Expose the dangers of broken and weak authentication methods and data leaking with poor or no encoding	• Use cross-site scripting (XSS) to execute code and the dangers of using Indirect Object References (IDOR)

CEHv10: Practical Web App Hacking	• Describe various methods of web app hacking and begin configuring web app hacking in a scenario • Continue configuring a web app hacking scenario	• Complete the configuration in web app hacking scenario
CEHv10: SQL Injection	• Describe SQL Injection attacks and use SQL Injection to bypass authentication on a Web App	
CEHv10: SQL Injection Types and Tools	• Describe error-based and blind SQL Injection attacks that can be used to enumerate database table and column information	• Use SQL Injection to read, write, and execute files on a remote system
CEHv10: Wireless Hacking Concepts	• Describe hacking wireless technologies concepts, define wireless terms, and recognize wireless standards, authentication mechanisms, and common encryption schemes	
CEHv10: Wireless Hacking Tools	• Use wireless hacking tools such as wireless adapters, antennas, and network discovery tools	• Use common wireless hacking tools such as Aircrack-ng Suite, Wifite, Fern Wifi Cracker, Cain&Abel, Kismet, WiFi Pineapple, WiFi-Pumpkin, and WiFi Jamming
CEHv10: Wireless Hacking Common Threats	• Recognize common threats against wireless networks like exploiting poorly configured devices, deploying Rogue APs, Evil Twin APs, Ad-hoc connections, and honeypot APs	• Recognize more complex wire network attacks such as MAC filter bypass by MAC spoofing and revealing hidden wireless networks
CEHv10: Cracking and Mobile Hacking	• Describe the process of cracking WEP encrypted wireless networks using the Aircrack-ng suite of wireless hacking tools • Describe the process of cracking WPA encrypted wireless networks using the Aircrack-ng suite of wireless hacking tools	• Describe hacking mobile devices, including mobile as an attack surface or platform, vulnerabilities found therein, and the realities of managing a BYOD environment
CEHv10: IoT Concepts	• Define the concept of IoT	• Describe IoT communication models and challenges associated with the use of IoT
CEHv10: IoT Attacks	• Describe IoT vulnerabilities	• Describe common IoT attack areas and threat
CEHv10: Cloud Computing Concepts	• Describe the concept of cloud computing, its key characteristics, and accepted service models	• Describe accepted cloud deployment models and cloud actors
CEHv10: Cloud Computer Attacks	• Describe cloud computing threats like insecure interfaces, malicious insiders, and more	• Describe cloud computer attacks like service and session hijacking, DNS attacks, SQL injection, and more
CEHv10: Cryptography Concepts	• Describe cryptography concepts and the goals of cryptography	• Describe cryptography concepts like digital signatures, symmetric cryptography, and asymmetric cryptography
CEHv10: Cryptography Concepts Part 2	• Describe cryptography concepts like cryptanalysis, cryptology, and collision	• Describe cryptography concepts like symmetric and asymmetric key algorithms and management

CEHv10: Cryptography Concepts Part 3	• Describe types of cryptosystems, hashing algorithms, and digital signatures	• Describe concepts like Public Key Infrastructure, digital certificates, certificate lifecycle, key wrapping, and Key Encrypting Keys
CEHv10: Cryptography Attacks	• Describe the various approaches that can be used to attack a cryptographic system	
CEHv10: IoT Hacking and Countermeasures	• Describe the IoT hacking methodology and common countermeasures for securing IoT devices	

Learn more at

www.hpe.com/ww/digitallearner

www.hpe.com/ww/digitallearner-contentpack

Follow us:

CP036, May 2019

Hewlett Packard Enterprise