CEH Exam Blueprint v2.0

EC-Council

Domains	Objectives	Weightage	Number of Questions
1. Background	• Networking technologies (e.g., hardware, infrastructure) • Web technologies (e.g., web 2.0, skype) • Systems technologies • Communication on protocols • Malware operations • Mobile technologies (e.g., smartphones) • Telecommunication on technologies • Backups and archiving (e.g., local, network)	4%	5
2. Analysis / Assessment	• Data analysis • Systems analysis • Risk assessments • Technical assessment methods	13%	16
3. Security	• Systems security controls • Application/file server • Firewalls • Cryptography • Network security • Physical security • Threat modeling • Verification procedures (e.g., false positive/negative validation) • Social engineering (human factors manipulation) • Vulnerability scanners • Security policy implications • Privacy/confidentiality (with regard to engagement) • Biometrics • Wireless access technology (e.g., networking, RFID, Bluetooth) • Trusted networks • Vulnerabilities	25%	31

4. Tools / Systems / Programs	• Network/host based intrusion • Network/wireless sniffers (e.g., WireShark, Airsnort) • Access control mechanisims (e.g., smart cards) • Cryptography techniques (e.g., IPsec, SSL, PGP) • Programming languages (e.g. C++, Java, C#, C) • Scripting languages (e.g., PHP, Java script) • Boundary protection appliances • Network topologies • Subnetting • Port scanning (e.g., NMAP) • Domain name system (DNS) • Routers /modems /switches • Vulnerability scanner (e.g., Nessus, Rena) • Vulnerability management and protection systems (e.g., Founds tone, Ecora) • Operating environments (e.g., Linux, Windows, Mac) • Antivirus systems and programs • Log analysis tools • Security models • Exploitation tools • Database structures	32%	40
5. Procedures / Methodology	• Cryptography • Public key infrastructure (PKI) • Security Architecture (SA) • Service Oriented Architecture • Information security incident • N-tier application design • TCP/IP networking (e.g., network routing) • Security testing methodology	20%	25
6. Regulation / Policy	• Security policies • Compliance regulations (e.g., PCI)	4%	5
7. Ethics	• Professional code of conduct • Appropriateness of hacking	2%	3

Validity: September 30th 2018