CEH Exam Blueprint v2.0

EC-Council

Section	Knowledge of:	Weight	Number of Questions
I. Background	A. networking technologies (e.g., hardware, infrastructure) B. web technologies (e.g., web 2.0, skype) C. systems technologies D. communication protocols E. malware operations F. mobile technologies (e.g., smart phones) G. telecommunication technologies H. backups and archiving (e.g., local, network)	4%	5
II. Analysis/Assessment	A. data analysis B. systems analysis C. risk assessments D. technical assessment methods	13%	16
III. Security	A. systems security controls B. application/file server C. firewalls D. cryptography E. network security F. physical security G. threat modeling H. verification procedures (e.g., false positive/negative validation) I. social engineering (human factors manipulation) J. vulnerability scanners K. security policy implications L. privacy/confidentiality (with regard to engagement) M. biometrics N. wireless access technology (e.g., networking, RFID, Bluetooth) O. trusted networks P. vulnerabilities	25%	31

Section	Knowledge of:	Weight	Number of Questions
IV. Tools / Systems / Programs	A. network/host based intrusion B. network/wireless sniffers (e.g., WireShark, Airsnort) C. access control mechanisims (e.g., smart cards) D. cryptography techniques (e.g., IPsec, SSL, PGP) E. programming languages (e.g. C++, Java, C#, C) F. scripting languages (e.g., PHP, Java script) G. boundary protection appliances H. network topologies I. subnetting J. port scanning (e.g., NMAP) K. domain name system (DNS) L. routers/modems/switches M. vulnerability scanner (e.g., Nessus, Retina) N. vulnerability management and protection systems (e.g., Foundstone, Ecora) O. operating environments (e.g., Linux, Windows, Mac) P. antivirus systems and programs Q. log analysis tools R. security models S. exploitation tools T. database structures	32%	40
V. Procedures / Methodology	A. cryptography B. public key infrastructure (PKI) C. Security Architecture (SA) D. Service Oriented Architecture E. information security incident F. N-tier application design G. TCP/IP networking (e.g., network routing) H. security testing methodology	20%	25
VI. Regulation/Policy	A. security policies B. compliance regulations (e.g., PCI)	4%	5
VII. Ethics	A. professional code of conduct B. appropriateness of hacking	2%	3