Network Security (for the Level 4 Network Engineer Apprenticeship)

9628-405 Network Security

Sample question paper answer sheet

Pass mark 21/30 (70%)

Question	ANSWER KEY	Test specification reference
1	d	1.1a Explain terminology for key IT security concepts Information assurance • CIA • Non repudiation
2	b	1.1b Explain terminology for key IT security concepts Information assurance • Threat • Vulnerability • Assets • Risk • Countermeasures
3	a	1.1c Explain terminology for key IT security concepts Information security
4	b	1.1d Explain terminology for key IT security concepts Information risk management
5	a	1.2a Describe vulnerabilities and threats associated with IT security Vulnerabilities • Physical access • User error • Malice • Firewall configuration • Password complexity • USB devices • OS/application patches • Coding errors
6	c	1.2a Describe vulnerabilities and threats associated with IT security Vulnerabilities (as above)
7	d	1.2b Describe vulnerabilities and threats associated with IT security Threats • Malware
8	d	1.2b Describe vulnerabilities and threats associated with IT security Threats • Malware

9	c	1.2c Describe vulnerabilities and threats associated with IT security Threats • Human behaviour • Hacking (brute force attack) • SPAM • Spoofing/man in the middle • Phishing • Spear phishing • Denial of service (DoS) • Distributed denial of service (DDoS)
10	b	1.2c Describe vulnerabilities and threats associated with IT security Threats (as above)
11	b	1.3a Explain risks management methods for different situations
12	a	1.3b Explain how to use risk calculation tools
13	c	1.4a Explain when to use IT security countermeasures and controls Environmental
14	c	1.4b Explain when to use IT security countermeasures and controls Technical
15	d	1.4c Explain when to use IT security countermeasures and controls Management (for procedural)
16	b	1.4d Explain when to use IT security countermeasures and controls Regulatory
17	d	2.1a Describe elements of network security that can be configured on a server to enhance security • System hardening
18	a	2.1b Describe elements of network security that can be configured on a server to enhance security • Virtual private networking • Firewall configuration • Intrusion detection/intrusion prevention (TRipwire/NIPS) • Anti-virus software • Spam filter • Enable and test system backups
19	d	2.1c Describe elements of network security that can be configured on a server to enhance security • Encryption
20	b	2.1d Explain the suitability of network security elements for different situations • System hardening

21	c	2.1d Explain the suitability of network security elements for different situations • System hardening
22	a	2.1e Explain the suitability of network security elements for different situations • Virtual private networking • Firewall configuration • Intrusion detection/intrusion prevention (TRipwire/NIPS) • Anti-virus software • Spam filter • Enable and test system backups
23	b	2.1f Explain the suitability of network security elements for different situations • Encryption
24	a	2.1f Explain the suitability of network security elements for different situations • Encryption
25	b	2.2 Explain suitability of tools and techniques used to identify vulnerabilities and threats
26	c	2.2 Explain suitability of tools and techniques used to identify vulnerabilities and threats
27	b	2.3 a Recommend appropriate incident response for information security incidents
28	c	2.3b Describe how to identify different instances and escalate in an appropriate way Incident responses lifecycle
29	c	2.3c Explain the suitability of network security elements for different situations • Incident identification • Escalation and notification • Mitigation steps • Recovery/reconstitution procedures.
30	c	2.3c Explain the suitability of network security elements for different situations • Incident identification • Escalation and notification • Mitigation steps • Recovery/reconstitution procedures.