Assignment Question Task 1 – 550 words Understand how computers and digital devices communicate with another over a network one. 1.1: Analyse the core vulnerabilities within a network environment and an online environment. 1.2: Explain how the emergence of security thinking and tools can benefit a network environment. Assessment Criteria 1.1: Analyse the core vulnerabilities within a network environment and an online environment. 1.2: Explain how the emergence of security thinking and tools can benefit a network environment. Task 2 – 350 words Understand, at a strategic level, how computer web applications and software can networking, be exploited. 2.1: Evaluate the link between network architecture and security engineering concepts. Assessment Criteria 2.1: Evaluate the link between network architecture and security engineering concepts. Task 3 – 550 words Understand methods of security prevention and systems hardening. 3.1: Evaluate internal risks and exposure. 3.2: Evaluate available process and physical defences against malicious network intrusions. Assessment Criteria 3.1: Evaluate internal risks and exposure. 3.2: Evaluate available process and physical defences against malicious network intrusions. Task 4 – 550 words Understand key network security and systems resilience tools, terminology and models. 4.1: Explain how key security concepts can be applied in a large and distributed organisation. 4.2: Assess how key factors are applied to enhance and embed an holistic approach to network and systems resilience. Assessment Criteria 4.1: Explain how key security concepts can be applied in a large and distributed organisation. 4.2: Assess how key factors are applied to enhance and embed an holistic approach to network and systems resilience.