

MARKING CRITERIA and STUDENT FEEDBACK

This section details the assessment criteria. The *extent* to which these are demonstrated by you determines your mark. The marks available for each criterion are shown. Lecturers will use the space provided to comment on the achievement of the task(s), including those areas in which you have performed well and areas that would benefit from development/improvement.

Common Assessment Criteria Applied	Marks Available	Marks Awarded
1. Engagement with Literature Skills		
While much of your research appears to be web-based, you have provided evidence of using a wide range of sources and materials in identifying and discussing the key concepts of the report. Your analysis of these sources is supported by clear endnotes and appropriate referencing following the desired IEEE method.	15	14
2. Knowledge and Understanding Skills		
While you have used a diverse array of sources that are clearly referenced and integrated into the report, I feel that several points were addressed in isolation, sometimes without clear connections back to the scenario provided. It would have been beneficial to emphasise the connections between key concepts such as the cyber kill chain, NIST framework and the mitigation strategies for malware and phishing attacks.	15	10
3. Cognitive and Intellectual Skills		
Your discussion on the different stages of the NIST framework in protecting against the cyber kill chain was thorough, but there was a lack of direct comparisons between stages, particularly regarding methods to prevent or identify attacks. This aspect could be improved upon in future analyses to demonstrate a clearer understanding. In your discussion of tools like Nmap and Wireshark for reconnaissance, the emphasis was primarily on their functions rather than how they could be utilized to exploit network weaknesses they uncover. Incorporating this aspect would enhance the practical applicability of the analysis. Regarding malware such as WannaCry and Telrat, while you provided mitigation strategies, they came across as somewhat generic. The report would have been improved by relating these strategies more closely to specific scenarios, identifying both common and unique approaches for mitigation. Although you explained phishing attacks like Whaling and Pharming, you missed discussing effective mitigation strategies for these risks.	20	10
4. Practical Application Skills		
You have successfully completed the Introduction to Packet Tracer and the final exam for Palo Alto Network Security Fundamentals and Cybersecurity Foundation. Your created topology demonstrates an appropriate use of design principles to mitigate single points of failure and ensure reliable crossover. You have failed to provide evidence of the methods to ensure the network is appropriately configured using technologies such as VLANs or protocols like Spanning Tree Protocol. Additionally, while you addressed software technologies, there was a lack of focus on hardware technologies and how they could be integrated into the provided topology.	40	25
5. Transferable Skills for Life and Professional Practice		
You have presented a professional report, covering all required content and effectively addressing the issues outlined in the scenario. It demonstrates a clear structure and adheres to the IEEE report format.	10	9

Assignment Mark (Assessment marks are subject to ratification at the Exam Board. These comments and marks are to give feedback on module work and are for guidance only until they are confirmed.)

Late Submission Penalties (tick if appropriate)

Up to four weeks late

1st/2nd/3rd attempt?

1st

68