## Aromatawai tuatoru | Assessment 3 – Outline

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | ‘Demonstrate a hack’ | **Total Possible Mark** | 100 |
| **Type** | Demonstration/Presentation | **Weighting** | 40% |
| **Learning Outcome(s)** | 1. Investigate OS, application, website and network threats and vulnerabilities 2. Investigate and implement OS, application, website and network security and testing techniques 3. Research tools and methods used in the IT industry related to cyber-attacks or cyber-security   INFO814   1. Analyse security threats and evaluate the possible consequences of security breaches 2. Critically assess the effectiveness of security countermeasures and forensic techniques 3. Recommend and justify a suitable information security system for a specific organisation | | |

### Task / Aim

Apply knowledge of cybersecurity principles to investigate a recent real-world security incident, analyse its vulnerabilities, and propose effective mitigation strategies.

Demonstrate cyber security skills through a practical demonstration of the hack or incident, highlighting its technical aspects and significant milestones.

### Conditions

* Can be done in pairs (two people)
* Duration: 10-15 minutes for the presentation, 5-10 minutes for the hack demo and 5 minutes for questions and discussions. (20-30 minutes total)
* Your group’s topic must be approved by your tutor by the end of week 4. All groups must have a unique topic.
* Your ‘hack’ demonstration can be a replication of part of the overall security incident your group is investigating. You must have tutor approval for the ‘hack’ component to ensure it is complex enough to cover the marking rubric.

### Task Details / Instructions / steps

1. Incident Selection: Choose a real-world security incident or hack that is of significant relevance in the cybersecurity domain. Ensure the incident is well-documented and from reputable sources. You may consider cybersecurity journals, industry reports, or reputable news outlets as sources for selecting the incident.
2. Incident Description: Clearly describe the chosen incident, providing relevant background information and explaining its impact on the affected entities or individuals. Present an overview of the incident, including the timeline and any significant events leading up to and following the incident.
3. Investigation of Threats and Vulnerabilities: Investigate and analyse the OS, application, website, and network threats and vulnerabilities that contributed to the security incident. Thoroughly research and evaluate the technical weaknesses exploited, considering aspects such as software vulnerabilities, misconfigurations, and network vulnerabilities.
4. Practical Demonstration: Develop a 5-10 minute hack demonstration that includes an interactive simulation or pre-recorded demonstration showcasing the hack. Clearly explain the process and milestones during the event, highlighting key points. Use visual aids, slides, or diagrams to support your presentation and enhance audience understanding. Consider technical requirements and ensure a consistent and effective demonstration experience. NOTE: if the hack demo is a video instead of a live demonstration, your mark will be capped at 74% for this section.
5. Fallout Analysis: Analyse the aftermath of the security incident, considering both immediate and long-term consequences from a technical perspective. Evaluate the impact on affected individuals, organisations, and the wider cybersecurity landscape. Consider factors like data breaches, system vulnerabilities, reputation damage, and potential legal or regulatory implications. Provide a comprehensive understanding of the incident's consequences.
6. Mitigation and Recommendations: Identify specific measures that could have been undertaken to handle the situation effectively from a cybersecurity professional's perspective. Recommend preventive and proactive measures to mitigate the identified vulnerabilities and minimise the risk of similar incidents in the future. Ensure your recommendations align with industry best practices and address the identified threats and vulnerabilities.
7. Extra INFO814 tasks:
   1. Examine the forensic response to the incident, evaluating the techniques and tools used. Discuss their effectiveness in uncovering critical information and their role in overall incident management.
   2. Assess the implemented security measures post-incident. Critically analyse their success in containing and mitigating the breach and discuss any shortcomings or areas for improvement.
   3. Suggest alternative forensic and security strategies that could have been more effective in this particular scenario, justifying these recommendations.
   4. Recommend changes to the organisation’s cyber structure, which must be undertaken to prevent a recurrence of similar incidents in the future. Keep in mind the financial and technological risks and costs involved in undertaking the recommendations and provide a clear logic for your recommendation(s).
8. Ethical Considerations: The presentation emphasises the ethical implications of discussing hacking techniques and security incidents. Highlight the importance of adhering to ethical standards and legal boundaries and respecting individuals' privacy rights. Provide specific examples of ethical boundaries and guidelines, such as responsible disclosure practices and avoiding disseminating sensitive information.
9. Presentation Guidelines: Prepare visual aids (slides, diagrams, etc.) to support your presentation. Ensure clarity, organisation, and effective communication of ideas. Use appropriate terminology and explain technical concepts in an understandable way to the audience. Engage the audience through clear explanations, real-world examples, and interactive elements when possible.

### Aromatawai tuatoru | Assessment 3 - Marking Rubric

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Exemplary  100-75% | Proficient  74-50% | Needs Improvement  49-0% |
| Incident Selection and Description 10% | The chosen incident is highly relevant. The description provides a comprehensive and precise overview of the incident, including relevant background information and a thorough explanation of its impact on the affected entities or individuals. The timeline and significant events leading up to and following the incident are accurately presented, demonstrating a deep understanding of the incident's context. | The chosen incident is relevant. The description provides relevant background information and adequately explains the incident's impact. The timeline and significant events are mostly accurate, demonstrating a good understanding of the incident's context. | The chosen incident is somewhat relevant. The description provides some background information and partially explains the incident's impact. The timeline and significant events may contain inaccuracies or be incomplete. |
| Investigation of Threats and Vulnerabilities 10% | The investigation demonstrates an exceptional understanding of threats and vulnerabilities related to the incident. The analysis is meticulous and comprehensive and covers both technical and business aspects in great detail. The vulnerabilities and weaknesses exploited are thoroughly evaluated, clearly explained, and supported by solid evidence. | The investigation demonstrates a solid understanding of threats and vulnerabilities related to the incident. The analysis provides sufficient detail and covers both technical and business aspects. The vulnerabilities and weaknesses exploited are adequately examined and explained with appropriate evidence. | The investigation demonstrates a partial understanding of threats and vulnerabilities related to the incident. The analysis lacks detail and may focus primarily on either technical or business aspects. The vulnerabilities and weaknesses exploited are partially examined and explained. |
| Practical Demonstration 40% | The practical demonstration successfully produces a working and fully functional demonstration of the hack or incident being researched. The demonstration accurately showcases the execution of the hack and its expected outcomes. The demonstration exhibits a deep understanding of the underlying techniques and vulnerabilities involved, with no significant issues or limitations. (Live demonstration) | The practical demonstration produces a working demonstration of the hack or incident being researched. The demonstration effectively showcases the execution of the hack and its expected outcomes. The demonstration demonstrates a solid understanding of the underlying techniques and vulnerabilities involved, with minor issues or limitations that do not significantly affect the demonstration's overall effectiveness. (Live or pre-recorded video of the hack) | The practical demonstration does not effectively produce a working demonstration of the hack or incident being researched. The demonstration may be incomplete, inaccurate, or fail to showcase the expected outcomes. The understanding of the underlying techniques and vulnerabilities involved may be insufficient or flawed, resulting in a demonstration that lacks functionality or fails to accurately represent the intended hack or incident. (Live or pre-recorded video of the hack) |
| Fallout Analysis 15% | The fallout analysis/evaluation provides a comprehensive understanding of the immediate and long-term consequences of the security incident. The impact on affected individuals, organisations, and the wider cybersecurity landscape is thoroughly discussed, considering factors such as extensive data breaches, critical system vulnerabilities, severe reputation damage, and complex legal or regulatory implications. | The fallout analysis/evaluation clearly explains the immediate and long-term consequences of the security incident. The impact on affected individuals, organisations, and the wider cybersecurity landscape is adequately discussed, considering factors such as data breaches, system vulnerabilities, reputation damage, and legal or regulatory implications. | The fallout analysis/evaluation lacks a proper understanding of the immediate and long-term consequences of the security incident. The impact on affected individuals, organisations, and the wider cybersecurity landscape is partially discussed, with limited consideration of factors such as data breaches, system vulnerabilities, reputation damage, and legal or regulatory implications. |
| Mitigation and Recommendations 15% | The mitigation and recommendations demonstrate an exceptional understanding of effective cybersecurity measures to handle the incident and prevent similar incidents in the future. The recommendations are practical, actionable, and aligned with industry best practices. The identified vulnerabilities are thoroughly addressed, and proactive measures are meticulously suggested. | The mitigation and recommendations demonstrate a solid understanding of effective cybersecurity measures to handle the incident and prevent similar incidents in the future. The recommendations are practical, actionable, and generally aligned with industry best practices. The identified vulnerabilities are adequately addressed, and some proactive measures are suggested. | The mitigation and recommendations demonstrate a partial understanding of effective cybersecurity measures to handle the incident and prevent similar incidents in the future. The recommendations may lack practicality, actionability, or alignment with industry best practices. The identified vulnerabilities are partially addressed, and few proactive measures are suggested. |
| Ethical Considerations 5% | The presentation consistently and persuasively emphasises the ethical implications of discussing hacking techniques and security incidents. The importance of adhering to ethical standards and legal boundaries and respecting individuals' privacy rights is effectively communicated throughout the presentation, with compelling examples and a profound understanding of responsible disclosure practices. | The presentation adequately emphasises the ethical implications of discussing hacking techniques and security incidents. The importance of adhering to ethical standards and legal boundaries and respecting individuals' privacy rights is mostly communicated throughout the presentation. | The presentation partially emphasises the ethical implications of discussing hacking techniques and security incidents. The presentation may not consistently communicate the importance of adhering to ethical standards and legal boundaries and respecting individuals' privacy rights. |
| Presentation 5% | The presentation flawlessly adheres to guidelines and demonstrates exceptional clarity, organisation, and effective communication of ideas. Visual aids (slides, diagrams, etc.) are meticulously prepared, supporting the presentation effectively. Technical concepts are explained with precision, clearly, and understandably. The overall delivery is engaging and confident and demonstrates outstanding presentation skills. | The presentation generally adheres to guidelines and demonstrates clarity, organisation, and effective communication of ideas. Visual aids (slides, diagrams, etc.) are adequately prepared, supporting the presentation. Technical concepts are explained clearly and understandably. The overall delivery is satisfactory and demonstrates a good command of presentation skills. | The presentation partially adheres to guidelines and needs more clarity, organisation, and effective communication of ideas. Visual aids (slides, diagrams, etc.) may be poorly prepared or not effectively support the presentation. Technical concepts may need to be clarified or adequately explained. The overall delivery lacks engagement and demonstrates weaknesses in presentation skills. |

### Extra INFO814 sections

Note: your grade for the previous sections will be scaled down to 70% and added to the 30% for the following sections.

| **Criteria** | **Exemplary (100-75%)** | **Proficient (74-50%)** | **Needs Improvement (49-0%)** |
| --- | --- | --- | --- |
| Examine the Forensic Response  7.5% | Demonstrates an in-depth critical evaluation of forensic response techniques and tools, explaining their effectiveness in uncovering critical information and their role in incident management. Comprehensive, well-researched, and insightful. | Provides a solid evaluation of forensic response techniques and tools, with reasonable analysis and explanation of effectiveness. Mostly complete with some insightful observations. | Shows basic or incomplete understanding of forensic response. The evaluation lacks depth and detailed analysis of the techniques and tools used. |
| Assess Post-Incident Security Measures  7.5% | Thoroughly assesses and critically analyses the success of security measures implemented post-incident, discussing both their strengths and shortcomings in detail. Offers well-rounded evaluation and improvement suggestions. | Adequately assesses security measures, identifying key strengths and weaknesses but may lack in-depth discussion of improvements. | Analysis of security measures is superficial or incomplete, with limited critique or suggestions for improvement. |
| Suggest Alternative Forensic and Security Strategies  7.5% | Provides well-justified recommendations for alternative forensic and security strategies, demonstrating a deep understanding of their potential effectiveness in the specific scenario. Detailed and well-reasoned justifications. | Suggests alternative strategies with reasonable justification, showing a good understanding of their relevance and potential effectiveness in the scenario. | Suggestions for alternative strategies are generic, poorly justified, or not well-aligned with the specific scenario. |
| Recommend Organisational Cyber Structure Changes  7.5% | Offers comprehensive, well-justified recommendations for changes to the organisation's cyber structure, considering financial and technological risks and costs. Clear, well-founded logic and thorough consideration of implications. | Provides solid recommendations with some justification, considering financial and technological aspects, but may lack depth or full consideration of implications. | Recommendations are vague, poorly justified, or do not adequately consider financial and technological aspects. Lack of clear logic or understanding of the implications of changes. |