Student Number: □

The University of Melbourne
Sample Exam

School of Computing and Information Systems

COMP90073 Security Analytics

Reading Time: 15 minutes.
Writing Time: 2 hours.
This paper has 6 pages including this cover page.
Common Content Papers: None

Authorised Materials: None. No calculators.

Instructions to Invigilators:
Each student should initially receive one standard script book.
Students must hand in **both** their **exam paper** and their **script book(s)**.
Students may **not** remove any part of the examination paper from the exam room.

Instructions to Students:

- This paper counts for 60% of your final grade, and is worth 60 marks in total.
- There are 15 questions, with marks as indicated. Attempt all questions.
- Answer questions 1–9 **on the exam paper**, and answer questions 10–15 on the lined pages in your **script book**. If you need more space for questions 1–9, then use the spare page at the end of the exam paper.
- Start your answer to each question in the script book on a new page.
- You must hand in **both** your **exam paper** and your **script book(s)**.
- Answer the questions as clearly and precisely as you can.
- Your writing should be clear. Unreadable answers will be deemed wrong. Excessively long answers or irrelevant information may be penalised.
- For numerical methods, marks will be given for applying the correct method. Students will not be heavily penalised for arithmetic errors.

Library: This paper may not be reproduced or held by the Baillieu Library.

Section A: Short Answer Questions (Write your answers on this page, and use your own words to provide a short description)

1. SYN flood is a Layer _____ DDoS attack and why?

   Answer:

2. Phishing is a popular _____ attack?

   (a) Man-in-the-Middle

   (b) Privilege Escalation

   (c) Social Engineering

   Answer:

3. What is the role of bottleneck in under-complete autoencoders?

   Answer:

4. Among the below windowing techniques choose the computationally efficient one(s). Choose all that apply.

   (a) Adaptive windows

   (b) Damped windows

   (c) Landmark windows

   (d) Sliding windows

   Answer:

5. In OCSVM one can calculate anomaly score for new sample z as $score(z) = \sum_{i=1}^{n} \alpha_i k(x_i, z) - \rho$. What would be the expected score of z if it is an anomalous sample?

Answer:

6. What is the purpose of indiscriminate evasion attacks?

Answer:

7. Give one scenario where the gradient-descent based method fails to generate an adversarial sample.

Answer:

8. Give two limitations of adversarial training.

Answer:

9. In indiscriminate attacks against reinforcement learning agents, the attacker maximises the cross-entropy loss in order to ____________________.

Answer:

Section B: Method and calculation Questions (Write your answers in your script book)

10. You are the security expert working for X Bank. Your main responsibility is to secure bank's Internet Banking system.

    (a) How do you maintain the confidentiality of information you need to protect?

    (b) What are two primary areas affecting the availability of your system?

11. Security firm Z-Tech designed a new software providing innovative solution to secure 5G networks, its Intellectual Property is worth \$5,000,000. The exposure factor is 70%, and the annualized rate of occurrence is 30%. What's the annualized loss expectancy?

12. In the lecture we covered 3 types of anomalies, (a) name these anomalies, (b) discuss their properties, (c) suggest an appropriate anomaly detection for each type, and justify your choice.

13. Recall that DBSCAN has two parameters, minPts and Eps. Suppose you apply DBSCAN to a dataset, but the clusters it produces are fragmented, i.e. the 'true' clusters you expect to see in the data are broken into multiple pieces by DBSCAN with parameters minPts and Eps. How could you change these parameters to reduce or eliminate this fragmentation?

14. Suppose that f is a binary linear classifier $f(x; W, b) = W \cdot x + b$, where $W = [2\ -1]$, $b = 0.5$, and $x = [x_1\ x_2]^T$, i.e., the input x is two dimensional. Given a point $x = [x_1\ x_2]^T$, it will be classified into Class 1 if $f(x) > 0$, or Class 2 otherwise. For example,

    (1) Since $f(2,\ 1) = [2\ -1][2\ \ 1]^T + 0.5 = 3 + 0.5 = 3.5 > 0$, the point $(2,\ 1)$ is classified into Class 1;

    (2) Since $f(-1,\ 1) = [2\ \ -1][-1\ \ 1]^T + 0.5 = -3 + 0.5 = -2.5 < 0$, the point $(-1,\ 1)$ is classified into Class 2.

    Generate an adversarial sample for point $(1, 7)$ using the iterative gradient sign method. The parameters in this algorithm are given as follows: (1) the step size is fixed to 1, (2) $\epsilon = 3$—the intermediate and final results need to be clipped if necessary, to make sure that they are in the $\epsilon-$neighbourhood of the original point, i.e., $|x_i - x_i'| \le \epsilon,\ i = 1, 2$.

15. Use automatic differentiation to calculate the partial derivative $\frac{\partial y}{\partial x_2}$ for $y = e^{x_1} - \frac{x_1}{x_2} + 2x_2$ at point $(3, 2)$.

Forward evaluation trace

$v_{-1} = x_1 = 3$

$v_0 = x_2 = 2$

$v_1 = e^{v_{-1}} = e^3$

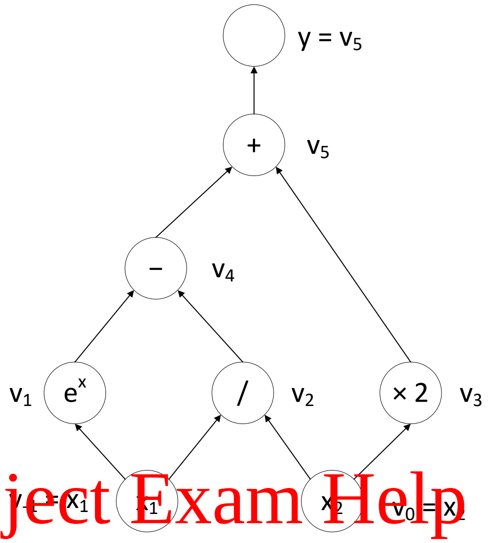
$v_2 = v_{-1}/v_0 = 1.5$

$v_3 = 2 \cdot v_0 = 4$

$v_4 = v_1 - v_2 = e^3 - 1.5$

$v_5 = v_3 + v_4 = e^3 + 2.5$

$y = v_5$



Forward derivative trace

$\dot{v}_{-1} = \dot{x_1} = 0$

$\dot{v}_0 = \dot{x_2} = 1$

$\dot{v}_1 =$ ________________

$\dot{v}_2 =$ ________________

$\dot{v}_3 =$ ________________

$\dot{v}_4 =$ ________________

$\dot{v}_5 =$ ________________

$\dot{y} = \dot{v_5}$

Reverse adjoint trace

$\bar{x}_1 = \bar{v}_{-1}$

$\bar{x}_2 = \bar{v}_0$

$\bar{v}_{-1} =$ ________________

$\bar{v}_0 =$ ________________

$\bar{v}_{-1} =$ ________________

$\bar{v}_0 =$ ________________

$\bar{v}_2 =$ ________________

$\bar{v}_1 =$ ________________

$\bar{v}_3 =$ ________________

$\bar{v}_4 = \bar{v}_5 \cdot \frac{\partial v_5}{\partial v_4} = 1$

$\bar{v}_5 = \bar{y} = 1$

END OF EXAM QUESTIONS

Extra space if needed to answer questions 1–9. If you write part of your answer here, please write the question number, and indicate at the corresponding question that you have used this space.

LAST PAGE OF EXAM