

程序代写代做 CS编程辅导



Wrap Up



WeChat: cstutorcs

Assignment Project Exam Help

COMP90073

Email: tutorcs@163.com
Security Analytics

QQ: 749389476

Sarah Erfani, Yi Han

CIS

<https://tutorcs.com>

Semester 2, 2021

程序代写代做 CS编程辅导

- Exam
- Subject revision
- Assignment feedback



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Exam Instructions

程序代写代做 CS编程辅导

- Wednesday 03/Nov, 3:00pm, LMS.
- Worth 60 marks, 30 marks reading time, 30 marks writing time.
- 15 minutes reading time, 30 minutes writing time.
- Answer all questions.



WeChat: cstutorcs

- Note that questions are not of equal value.
- 2–3 sentences sufficient for when brief descriptive answer requested.
- Please use your script book for the long answer question, clearly marking where the response starts. Any pages which are not labelled as forming part of the response to that question number will not be considered during marking.
- A sample exam will be available soon.

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Types of Questions

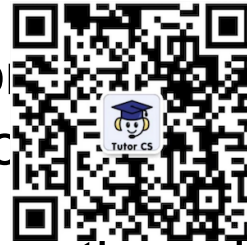
程序代写代做 CS编程辅导

There are a mix of question types on the exam.

- **Conceptual:** A question which tests or requires you to define or explain a concept, term, or algorithm introduced in the subject.
- **Problem solving:** A question which asks you to use a specific algorithm or formula to solve a problem on some data.
- **Application:** A question which asks you to demonstrate that you have gained a high-level understanding of the methods and algorithms covered in this subject, and can apply that understanding.

QQ: 749389476

<https://tutorcs.com>



WeChat: estutores

Assignment Project Exam Help

Email: tutorcs@163.com

A Comment on Mathematical Concepts

程序代写代做 CS编程辅导

We expect you to be able to do:

- Remember simple, key
- Read and understand n complex formulas that have been presented for core concepts, provided “bare”.



WeChat: cstutorcs

- E.g., attacker’s objective functions in adversarial attacks against machine learning models

Assignment Project Exam Help

- Addition, subtraction, multiplication, division
- Reducing and ordering of fractions
- Gradient-descent based method for generating adversarial samples

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Week 1: Introduction to Cybersecurity & Security Analytics Use Cases and Data

程序代写代做 CS编程辅导

- Core cyber security principle
 - Explain CIA triad
 - Apply the appropriate controls to protect CIA



- Key access control concepts
 - Describe access control and four key attributes
 - Explain “Defense in Depth”

WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

- Security analytics use cases and data
 - Explain seven common use cases

QQ: 749389476

<https://tutorcs.com>

– Explain four data sources

程序代写代做 CS编程辅导

- Cyber Kill Chain

- Explain seven steps of kill chain



- Model cyber attacks using cyber kill chain

WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

- Fundamentals of Networking Protocols
 - Understand DHCP protocols and TCP three-way handshake
- Network Attacks
 - Compare different types of attacks
 - Understand how network attacks work
 - Describe examples of different types of attacks
- Network Security Systems
 - Explain DMZ and network segmentation
 - Explain NAT & PAT process
 - Compare the difference between IDS and IPS

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Week 4: Botnet & DDoS Deep Dive & Business Context for Cybersecurity Management

程序代写代做 CS编程辅导

- Botnet Deep Dive

- Explain phases of botnet life cycle
- Compare the differences between push and pull based propagation methods



WeChat: cstutorcs

- DDoS Deep Dive

- Compare three types of DDoS attacks

Assignment Project Exam Help

Email: tutorcs@163.com

- Information Security Management Governance

- Determine qualitative risks
- Calculate quantitative risks

QQ: 749389476

<https://tutorcs.com>

Week 5: Intro to Anomaly Detection, Clustering and Density-based methods

程序代写代做 CS编程辅导

- Describe shortcomings of convectional security systems

- Discuss the objective and detection

- Define different types of files



- Discuss operation of iForest, and describe the advantages of this method

WeChat: cstutorcs

- Apply clustering algorithms to identify anomalies

Email: tutorcs@163.com

- Discuss differences between distance and density based methods

QQ: 749389476

<https://tutorcs.com>

Week 6: Anomaly Detection in Evolving Data Streams

程序代写代做 CS编程辅导

- Characterise the differences between batch and incremental learning
- Describe the operation and properties of HS-tree algorithm
- Describe an efficient approach to extend LOF to incremental learning



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Week 6: Anomaly Detection Using Support Vector Machine

程序代写代做 CS编程辅导

- Describe the operation of SVDD/OCSVM
- Characterise the key parameters of SVDD/OCSVM
- Derive the dual formulation of SVDD/OCSVM from the primal formulation



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Describe operation and training of autoencoder

- Identify anomalies using autoencoder



- Characterise properties of different types of autoencoders

WeChat: cstutorcs

- Characterise the key parameters different autoencoders' loss function

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Graphs cannot always be treated as points lying in a multi-dimensional space independently.
- Preserve data structure
- Characterise the properties of random walk and graph convolutional network
- Apply graph embedding for anomaly detection



WeChat: estutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Week 8: Contrast Mining

程序代写代做 CS编程辅导

- Explain the advantage of contrast mining in cybersecurity problems
- Compare and contrast algorithms on different datasets
- Find frequent patterns using FP-Growth algorithm



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Week 9: Adversarial Machine Learning – Vulnerabilities (Part I)

程序代写代做 CS编程辅导

- Evasion attacks

- Indiscriminate: $\arg \min_{\delta \in [0,1]} c \cdot f_{true}(x + \delta)$
- Targeted: $\arg \min_{\delta \in [0,1]} c \cdot f_{target}(x + \delta)$
- Gradient-descent based approach to generate adversarial samples
- Automatic differentiation

WeChat: cstutorcs

- Poisoning attacks

Assignment Project Exam Help

- Attacker's objective: $O_A(D, \hat{\theta}_D) = \|\hat{\theta}_D - \theta^*\| + \|D - D_0\|_2$
- $\hat{\theta}_D (\theta^*)$: parameter of the poisoned (targeted) model
- $D (D_0)$: poisoned (original) training dataset

Email: tutorcs@163.com

QQ: 749389476

- Transferability

<https://tutorcs.com>

- Black-box attacks

- Adversarial attacks in domains other than computer vision (malware detection)
- Potential locations of adversarial examples
 - Off the data manifold
 - Sparse data
- Why are machine learning models vulnerable?
 - Insufficient training data
 - Unnecessary features
- How to defend against adversarial machine learning?
 - Data-driven defences
 - Filtering adversarial samples
 - Adversarial training
 - Project to lower dimension
 - Learner robustification
 - Distillation
 - Stability training
 - Adaptive attackers

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Reinforcement learning

- State, action, reward
- Value function, policy
- Q-learning → Q-network → DDQN



- Adversarial reinforcement learning

- Manipulate the states observed by the agent
- Cross entropy loss: $J = -\sum_i p_i \log \pi_i$

- π_i : probability of taking action a_i

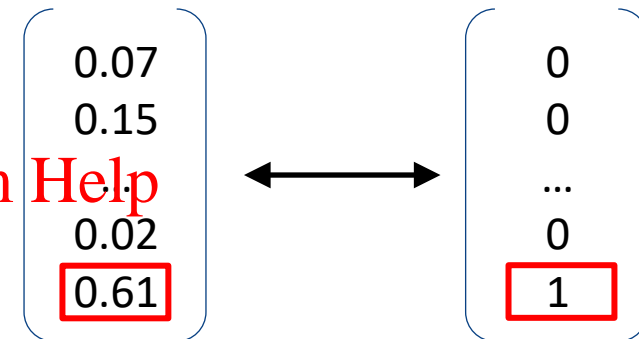
- $p_i = \begin{cases} 1, & \text{if } a_i = \text{optimal action} \\ 0, & \text{otherwise} \end{cases}$

- Maximise $J \rightarrow$ minimise the probability of taking the optimal action

- Test time/training time

- Timing of the attack <https://tutorcs.com>

- Defence – adversarial training



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

程序代写代做 CS编程辅导

- No examinable material



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Wrapping Up

程序代写代做 CS编程辅导

- I hope you enjoyed this introduction to security analytics
- Maybe we'll see you in programs
- Thank you for your patient attention



WeChat: estutorcs

- Good luck with your exams and future studies

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>