قائمة الاسئلة

الذكاء الاصطناعي للامن السيبراني - المستوى الثالث -قسم الامن السيبراني - - كلية الحاسوب وتكنولوجيا المعلومات - الفترة - درجة الامتحان (40

ا.د. غالب الجعفري

1) What is Machine Learning (ML)?
   1) - A technology that requires explicit programming for decision-making.
   2) + A method that enables systems to learn patterns and make decisions from data without explicit programming.
   3) - A manual coding process that does not involve data.
   4) - A method that relies solely on human intuition and does not use data.
2) What are the main types of Machine Learning (ML)?
   1) + Supervised Learning,Clustering and Reinforcement Learning
   2) - Supervised Learning,Unsupervised Learning and Reinforcement Learning
   3) - Supervised Learning,Genetic Algorithms and Reinforcement Learning
   4) - Supervised Learning,Classification and Reinforcement Learning
3) What does Representation in Cybersecurity refer to?
   1) - How physical security measures are implemented in the cybersecurity domain.
   2) + How data is structured and features are defined for machine learning models in the cybersecurity domain.
   3) - How user interfaces are designed for cybersecurity software.
   4) - How network devices are configured in the cybersecurity domain
4) Which of the following are common features used in cybersecurity for machine learning models?
   1) + IP addresses, timestamps, port numbers.
   2) - Social media profiles and follower counts.
   3) - Music preferences and listening habits.
   4) - Shopping history and purchase amounts.
5) Which of the following features are commonly used to detect phishing emails that trick recipients into providing sensitive information?
   1) - Normal sender email addresses
   2) - Frequent sender email addresses
   3) - Recognized sender email addresses
   4) + Language patterns in the email body
6) What is Model Fitting in the context of cybersecurity?
   1) - The process of deploying a machine learning model to live environments without any adjustments.
   2) + The process of training a machine learning model to learn patterns in cybersecurity data by adjusting its parameters to minimize errors.
   3) - The process of visualizing cybersecurity data without using any machine learning techniques.
   4) - The process of creating manual rules for cybersecurity systems without using machine learning.
7) What is the goal of training a machine learning model to distinguish between benign and malicious network traffic using labeled data?
   1) - To create manual rules for classifying network traffic.
   2) - To deploy a model without using any labeled data.
   3) + To fit a model to classify new traffic accurately by learning from traffic logs labeled as "benign" or "malicious."
   4) - To visualize network traffic data without any classification.
8) What does Prediction in Cybersecurity involve?
   1) - Using a manual process to identify threats in known data.
   2) + Using a trained model to identify threats, anomalies, or malicious activity in new, unseen data.
   3) - Using random methods to generate predictions without any model.

4) - Using a model to simulate physical security measures.

9) What does Generalization in Cybersecurity refer to?
1) - The ability of a model to memorize specifics from the training data and perform well only on that data.
2) + The ability of a model to perform well on unseen cybersecurity data, ensuring it captures underlying patterns rather than memorizing specifics from the training data.
3) - The ability of a model to visualize cybersecurity data without any training.
4) - The ability of a model to simulate physical security measures in a network.

10) What are some common challenge in achieving generalization for machine learning models in cybersecurity?
1) + Rapidly evolving threats (e.g., new malware variants)
2) - Limited computational power
3) - Slow network speeds
4) - Infrequent updates to models

11) What is overfitting in the context of cybersecurity machine learning models?
1) + A complex model might memorize specific attack data, failing to generalize to new threats.
2) - A model might perform well on new threats but fail to memorize specific attack data.
3) - A model might ignore specific attack data, generalizing well to new threats.
4) - A complex model might generalize well to new threats but fail to learn specific attack data.

12) What is underfitting in the context of cybersecurity machine learning models?
1) - A complex model might memorize specific attack data, failing to generalize to new threats.
2) + A simple model might miss subtle attack patterns, failing to learn and identify them.
3) - A model might perform well on new threats but fail to memorize specific attack data.
4) - A model might ignore specific attack data, generalizing well to new threats.

13) What forms the foundation of Machine Learning (ML) in cybersecurity?
1) - User interface designs and visual elements.
2) - Physical security measures and hardware configurations.
3) + Data, which includes logs, traffic, and other indicators of malicious or benign activities.
4) - Human intuition and manual coding processes.

14) Why is evaluating the performance of a machine learning model crucial?
1) + to measure both the training error (empirical error) and the generalization error (true error).
2) - To measure only the training error (empirical error) and ignore the generalization error (true error).
3) - To measure the physical dimensions of the model.
4) - To measure the visual appearance of the model.

15) What does the empirical error (training error) indicate in machine learning?
1) - The average difference between the predicted value and the true value in the test dataset.
2) + The average loss over the training dataset, indicating how well the model fits the training data.
3) - The overall performance of the model in real-world scenarios.
4) - The computational time required to train the model.

16) What does stability refer to in the context of machine learning models?
1) - A model's ability to process data faster.
2) + A model's consistency in producing similar predictions for slightly different datasets.
3) - A model's capability to handle large datasets.
4) - A model's flexibility in changing parameters without losing accuracy.

17) Which of the following are not characteristics of stable models in machine learning?
1) - Low sensitivity to small changes in training data
2) - Robustness to noise and outliers
3) - Linear regression is typically stable
4) + High sensitivity to large changes in training data

18) What is the purpose of regularization in machine learning models?

1) - Increasing the complexity of the model to fit the training data better.
2) + Preventing overfitting by adding a penalty term to the model's loss function.
3) - Reducing the training time by simplifying the model's architecture.
4) - Enhancing the visual representation of the model's predictions

19) What is the primary focus of discriminative models in machine learning?
1) - Learning the underlying distribution of the features without considering the labels.
2) + Learning the boundary between classes by modeling the probability of the label given the features.
3) - Generating new data samples based on the distribution of the training data.
4) - Reducing the dimensionality of the feature space without considering the labels.

20) What is the primary focus of generative models in machine learning?
1) - Modeling the boundary between classes without considering the data distribution.
2) + Learning the underlying distribution of the data by modeling P(X□Y)P(X|Y) (how features are distributed for each label) and P(Y)P(Y) (prior probabilities of labels) to indirectly calculate P(Y□X)P(Y|X).
3) - Reducing the dimensionality of the feature space without considering the labels.
4) - Generating new data samples based on the boundary between classes.

21) What is the primary aim of discriminative models in machine learning?
1) - To model the overall data distribution without considering the conditional probabilities.
2) + To estimate the conditional distribution P(Y□X)P(Y|X) where YY is the label and XX is the feature set.
3) - To generate new data samples based on the distribution of the training data.
4) - To reduce the dimensionality of the feature space without considering the labels.

22) What is the primary aim of generative models in machine learning?
1) - To estimate the conditional distribution P(Y□X)P(Y|X) where YY is the label and XX is the feature set.
2) + To model the underlying data distribution by estimating the joint distribution P(X,Y)P(X,Y).
3) - To reduce the dimensionality of the feature space without considering the labels.
4) - To visualize the data distribution without any modeling.

23) Which of the following statements is true about conditional and joint distributions?
1) - You can derive the joint distribution from the conditional distribution, but not vice versa.
2) + You can derive the conditional distribution from the joint distribution, but not vice versa.
3) - Conditional and joint distributions are independent of each other.
4) - You cannot derive one from the other in any case.

24) Which of the following is not example of discriminative models in machine learning?
1) - Logistic Regression
2) - Support Vector Machines (SVM)
3) - Conditional Random Fields (CRFs)
4) + Gaussian Mixture Models

25) What is the purpose of creating models to understand how people create passwords?
1) - To randomly guess passwords without any pattern.
2) + To predict the kinds of passwords people might choose by identifying patterns or rules.
3) - To visualize the physical characteristics of passwords.
4) - To enhance the aesthetic design of password entry fields.

26) What happened during the LinkedIn database leak in 2012?
1) - Over 160 million user emails were leaked.
2) + Over 160 million user passwords were leaked.
3) - Over 160 million user profile pictures were leaked.
4) - Over 160 million user messages were leaked.

27) What happened during the Adobe database leak in 2013?

1) - 153 million user profile pictures were leaked, including encrypted passwords.
2) + 153 million user records were leaked, including encrypted passwords.
3) - 153 million user emails were leaked, excluding encrypted passwords.
4) - 153 million user messages were leaked, including encrypted passwords.

28) What strategy do attackers often use to guess passwords?
1) - Start by guessing the most uncommon or unlikely passwords before trying random ones.
2) + Start by guessing the most common or likely passwords before trying random ones.
3) - Randomly guess passwords without any specific strategy.
4) - Only guess passwords based on physical characteristics.

29) Which common passwords are often tried first by attackers?
1) - Passwords with complex characters and symbols.
2) + Common passwords like "password," or "qwerty."
3) - Common passwords like "password," or "qwrety."
4) - Passwords with a mix of upper and lower case letters.

30) What do attackers typically do when they gain access to password hashes (like bcrypt hashes) from a compromised database?
1) + Attempt to reverse-engineer or "crack" these hashes by making password guesses, hashing them, and comparing the results with the database entries.
2) - Immediately delete all password hashes to prevent further use.
3) - Encrypt the password hashes with an additional layer of security.
4) - Share the password hashes publicly without any further action.

31) What is the typical process attackers use to crack bcrypt password hashes?
1) - The attacker generates guesses (passwords), encrypts them with a different algorithm, and compares the results with the database hash.
2) + The attacker generates guesses (passwords), hashes them using bcrypt, and compares the result with the database hash.
3) - The attacker generates random strings, converts them to plaintext, and compares the results with the database hash
4) - The attacker generates guesses (passwords), decrypts the database hash, and compares it with the plaintext passwords.

32) What is credential stuffing in the context of cybersecurity?
1) - The attacker generates random strings and tries them on various websites.
2) - The attacker encrypts new passwords and replaces the original ones in the database.
3) + The attacker takes the cracked password and tries it on other websites where the same user may have an account.
4) - The attacker deletes all user accounts from the database.

33) What does a password-strength metric measure, and what does parameterized guessability refer to?
1) - The visual appeal of a password; the ease of remembering it.
2) - The number of characters in a password; the time taken to input it manually.
3) + How resistant a password is to cracking attempts by attackers using automated guessing algorithms; estimating the number of guesses required to correctly identify a given password under specific conditions.
4) - The frequency of password reuse; the number of different algorithms used to guess a password.

34) What is an attacker's first step when they compromise a database and see bcrypt password hashes like $2a$04$iHdEgkI681VdDMc3f7edau9phRwORvhYjqWAIb7hb4B5uFJO1g4zi?
1) - Encrypt the database with a different algorithm.
2) - Publicly share the hashed passwords without any further action.
3) + Attempt to reverse-engineer or "crack" these hashes by making password guesses, hashing them using bcrypt, and comparing the results with the database entries.

4) - Immediately delete all password hashes to prevent further use.

35) What is the primary difference between Narrow AI and Artificial General Intelligence (AGI)?
1) - Narrow AI is designed to perform a wide range of tasks, while AGI focuses on specific tasks.
2) - AGI is used only for gaming purposes, while Narrow AI is used in all other domains.
3) - AGI is limited to data analysis, while Narrow AI can perform human-like cognitive abilities.
4) + Narrow AI is designed to perform a specific task, such as voice recognition or data analysis, while AGI aims to replicate human-like cognitive abilities.

36) What does ensuring availability in the context of system design and cybersecurity mean?
1) - Preventing unauthorized access to systems and data.
2) - Encrypting data to protect it from being read by unauthorized users.
3) + Ensuring that systems and data are available when needed.
4) - Monitoring system performance to improve efficiency.

37) How does AI contribute to threat detection in cybersecurity?
1) - AI can randomly generate passwords for users.
2) - AI can only monitor system performance to improve efficiency.
3) + AI can identify unusual patterns in network traffic and system behavior, helping to detect potential threats in real-time.
4) - AI can encrypt data to protect it from being read by unauthorized users.

38) How does predictive analytics contribute to cybersecurity?
1) - By randomly generating passwords for users.
2) - By monitoring system performance to improve efficiency.
3) + By analyzing historical data to predict potential vulnerabilities and security breaches.
4) - By encrypting data to protect it from being read by unauthorized users.

39) How does AI help protect cloud infrastructures in terms of security?
1) - By randomly generating passwords for cloud users.
2) + By monitoring and analyzing large amounts of data to detect abnormal activity.
3) - By manually inspecting each cloud server for potential vulnerabilities.
4) - By encrypting all data stored in the cloud.

40) Why has AI been integrated into cybersecurity to predict, detect, and mitigate threats in real-time?
1) - Because cyberattacks are becoming less frequent and less complex.
2) - Because AI can manually inspect each system for vulnerabilities.
3) + Because the growing complexity of cyberattacks has prompted the need for advanced tools to predict, detect, and mitigate threats in real-time.
4) - Because AI can encrypt all data stored in the cloud.