### Definitions

### Network intrusion detection system contains sensors that can detect that an attack was launched against a particular host computer. It does not record the source Internet Protocol (IP) address.

### File integrity checking software logs can detect changes to important files using a checksum software that counts the total number of bits in a file to determine whether a file's size was changed. It does not record the source Internet Protocol (IP) address.

### Application software logs can document changes that occurred to a specific application software, such as an accounts payable system. It does not record the source Internet Protocol (IP) address.

### The standard error of the estimate is a measure of the accuracy of predictions.

### Chi-square test is used for testing the independence of the two variables and testing hypotheses concerning proportions in a population. The upper tail of the Chi-square distribution is used to determine whether an observed pattern of frequencies is different from an expected pattern of frequencies. The calculated value of the Chi-square statistic will be close to zero when the observed frequencies are very close to the expected frequencies. On the other hand, the calculated static will be more than zero when the difference between these two frequencies is larger.

### Logistic regression is a statistical model that in its basic form uses a logistic function to model a binary dependent variable, although many more complex extensions exist. In regression analysis, logistic regression (or logit regression) is estimating the parameters of a logistic model (a form of binary regression).

### C:\Users\Kanishka Prasad\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\63D91650.tmp

### Decision tree is a decision support tool that uses a tree-like model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. It is one way to display an algorithm that only contains conditional control statements. A decision tree is a flowchart-like structure in which each internal node represents a "test" on an attribute (e.g. whether a coin flip comes up heads or tails), each branch represents the outcome of the test, and each leaf node represents a class label (decision taken after computing all attributes).

### Exponential smoothing is a rule of thumb technique for smoothing time series data using the exponential window function. Whereas in the simple moving average the past observations are weighted equally, exponential functions are used to assign exponentially decreasing weights over time.

### Dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.

### Skimming is a method used by identity thieves to capture information from a cardholder.

### Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

### Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they use to try and steal their victims' personal information.

### Coefficient of determination is a measure used in statistical analysis that assesses how well a model explains and predicts future outcomes.

### Correlation coefficient is a statistical measure that calculates the strength of the relationship between the relative movements of two variables. The values range between -1.0 and 1.0. A calculated number greater than 1.0 or less than -1.0 means that there was an error in the correlation measurement.

### False rejection rate is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user.

### False acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

### Null hypothesis is a general statement or default position that there is nothing significantly different happening, like there is no association among groups or variables, or that there is no relationship between two measured phenomena.

### Type I error is the rejection of a true null hypothesis (nothing is wrong or diff from normal behaviour between variables) as the result of a test procedure. Type I error, called false rejection rate, is incorrect because genuine users are rejected as imposters. A goal of biometrics-based identification and authentication techniques about biometric errors is to obtain low numbers for both false rejection rate and false acceptance rate errors.

### Type II error is the failure to reject a false null hypothesis (nothing is wrong or diff from normal behaviour between variables) as the result of a test procedure. Type II error, called false acceptance rate, is incorrect because imposters are accepted as genuine users. A goal of biometrics-based identification and authentication techniques about biometric errors is to obtain low numbers for both false rejection rate and false acceptance rate errors.

### Crossover error rate describes the point where the false reject rate (FRR) and false accept rate (FAR) are equal. ... The crossover error rate describes the overall accuracy of a biometric system.

### False non-match rate (FNMR) is the rate at which a biometric matcher miscategorises two captures from the same individual as being from different individuals. False non-match rate is an alternative to false rejection rate. It is used to avoid confusion in applications that reject claimants if their biometric data matches with that of an applicant.

### Pharming attack: Internet-related threats are broken down into three categories: browser-based, server-based, and network-based attacks. Pharming attack is an example of network-based attack. An attacker may modify the domain name system (DNS) mechanism to direct it to a false website. These techniques are often used to perform pharming attacks, where users may divulge sensitive information. Note that pharming attacks can also be initiated by subverting the victim's host computer files.

### Masquerading attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.

### Custom code injection is an example of server-based attack. Attackers can inject custom code into the website for subsequent browsers to process via cross-site scripting (XSS) software. Subtle changes introduced into the web server can radically change the server’s behavior (e.g., turning a trusted entity into malicious one), the accuracy of the computation (e.g., changing computational algorithms to yield incorrect results), or the confidentiality of the information (e.g., disclosing collected information).

### Economies of scope refers to gaining efficiencies with the integration of the number of products, services, systems, functions, and activities in an organization. For example, integrating financial systems with nonfinancial systems is an example of economies of scope. Similarly, integrating all business functions such as manufacturing, marketing, accounting, finance, and human resources is another example of economies of scope. Basically, economies of scope refers to the ability of a firm to produce multiple products or render multiple services more inexpensively in combination than separately.

### Wiretapping is a computer crime. An unauthorized device is attached to a telecommunications circuit for the purpose of obtaining active and/or passive access.

### Eavesdropping is a computer crime involving an unauthorized interception of information. It is the act of secretly or stealthily listening to the private conversation or communications of others without their consent.

### Super-zapping, a utility program in the IBM mainframe computer environment, can be thought of as the master key to the computer system. It unlocks most of the security safeguards and integrity controls. In the wrong hands, its use can be damaging. Use of supervisor privileges, root privileges, or the running of programs that bypass security controls is needed to troubleshoot certain operating system problems. In other words, super-zapping can be used for both good and bad purposes. The problem is that no audit trail exists.

### Malvertizing attack is the use of malicious advertisements (ads) on legitimate websites. These ads contain a programming code that will infect a user's computer without any action required from the user (i.e., the user does not have to click on the ad to become infected).

### Adware is any software program intended for marketing purposes, such as to deliver and display advertising banners or pop-ups to the user's computer screen or to track the user's online usage or purchasing activity. Adware tracks a user's activity and passes it to third parties without the user's knowledge or consent. Click fraud is possible with adware because it involves deceptions and scams that inflate advertising bills with improper usage and charges per click in online web advertisements.

### Scanning attack is sending network packets or requests to another system to gain information to be used in a subsequent attack.

### Skimming attack is the unauthorized use of a reader to read tags without the authorization or knowledge of the tag's owner or the individual in possession of the tag. An example of a skimming attack is on radio frequency identification (RFID) tags. A security control is to install anti-skimming material using electromagnetic shields.

1. **Stem-Leaf Diagram:** SL diagram is a major technique used in exploratory data analysis as it shows measurements in a rank-ordered bar chart format. This diagram is similar to a histogram but is relatively easier to develop. The diagram shows individual values whereas the histogram shows groups of defined classes. The diagram is appropriate to use only when the first-digit or the first two-digits provide a good basis for separating data into groups. Each group then is similar to a class or category in a frequency distribution. For example, the first-digit represents the stem and each of the measurements associated with the first-digit values becomes a leaf in the display.

### Image result for stem and leaf diagram

### MongoDB Database is designed to support humongous databases. It's a NoSQL database with document-oriented storage, full index support, replication, and high availability.

### Oracle Database v11 is a Relational Database Management System (RDBMS). RDBMSs are schema-oriented, which means the structure of the data should be known in advance to ensure that the data adheres to the schema.

###  Database system recovery:

### Rollback restores the database from one point in time to an earlier point. This feature can help in database recovery efforts.

### Rollforward restores the database from a point in time when it is known to be correct to a later time. This feature can help in database recovery efforts.

### Gantt chart is a graphical illustration of a scheduling technique. The structure of the chart shows output plotted against units of time. It does not include cost information. It highlights activities over the life of a project and contrasts actual times with projected times using a horizontal (bar) chart. It gives a quick picture of a project's progress in terms of actual time lines and projected time lines. The Gantt chart looks like a bar chart. The Gantt chart is used for milestone scheduling where each milestone has start and completion dates. A milestone represents a major activity or task to be accomplished (e.g., design phase in a computer system development project).

### Static code analysis is a method of debugging by examining source code before a program is run. It’s done by analysing a set of code against a set (or multiple sets) of coding rules. Static code analysis and static analysis are often used interchangeably, along with source code analysis.

### Radar chart is a visual method to show in graphic form the size of gaps in a number of areas such as current performance versus ideal (expected) performance and current budget versus previous budget.

### C:\Users\Kanishka Prasad\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5B196375.tmp

### Box plot/whisker Daigram is a graph showing the distribution of a dataset measuring data variability at the quartiles and interquartile range. It is easier to graph than a histogram as it observes the extent of skewness in the data distribution. The box plot is also called a box-and-whisker plot and is the main technique of exploratory data analysis. An example of a box plot application is distribution of patient treatment length in time for each type of treatment category of health services.

### C:\Users\Kanishka Prasad\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\88321A4B.tmp

### Pareto charts can be drawn to separate the "vital few" items from the "trivial many" items. It is based on the 80/20 rule, that is, 20% of items contribute to 80% of problems. It is a problem-solving tool. The Pareto chart looks like a pie chart but they are not the same.

### Image result for pareto chart

### Part-to-whole chart shows the percentage of a part in relation to its whole. For example, a retailer's marketing department can conduct a part-to-whole demographic analysis to show how customers’ age group is distributed in each market region such as south, north, east, and west.

### Related image

### Decision tables: are a concise visual representation for specifying which actions to perform depending on given conditions. They are algorithms whose output is a set of actions. The information expressed in decision tables could also be represented as decision trees or in a programming language as a series of if-then-else and switch-case statements.

###

### Contingency table/ cross tabulation / Crosstab: A contingency table is a type of table presented in a matrix format displaying frequency distribution, showing their probabilities. Contingency tables (cross-tabulations) are used in business intelligence, market research, and customer surveys where interrelations and interactions between two or more variables can be studied to obtain greater insights of data. Due to their statistical focus, contingency tables show a measure of association between variables. For example, a table can be put together showing how male and female customers prefer to purchase product A and product B from a retailer.

### C:\Users\Kanishka Prasad\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4722572.tmp

### Deterrent controls: are designed to discourage those who might seek to violate our security controls from doing so, whether the threat is external or internal, it discourages the same type of activities.

### Query by Example (QBE) is a database query language for relational databases. It is the first graphical query language, using visual tables where the user would enter commands, example elements and conditions. Many graphical front-ends for databases use the ideas from QBE today. Originally limited only for the purpose of retrieving data, QBE was later extended to allow other operations, such as inserts, deletes and updates, as well as creation of temporary tables. The user can submit a document, or several documents, and ask for "similar" documents to be retrieved from a document database.

### Ad hoc query is a loosely typed command/query whose value depends upon some variable. Each time the command is executed, the result is different, depending on the value of the variable. It cannot be predetermined and usually comes under dynamic programming SQL query. An ad hoc query is short lived and is created at runtime.

### Online analytical processing, or OLAP is an approach to answer multi-dimensional analytical (MDA) queries swiftly in computing.[1] OLAP is part of the broader category of business intelligence, which also encompasses relational databases, report writing and data mining.[2] Typical applications of OLAP include business reporting for sales, marketing, management reporting, business process management (BPM),[3] budgeting and forecasting, financial reporting and similar areas, with new applications emerging, such as agriculture. OLAP performs multidimensional analysis of business data and provides capability of complex calculations.

### Grid computing is a form of distributed computing whereby a super-virtual computer is composed of many networked and loosely coupled computers working together to perform very large tasks. The grid handles non-interactive workloads that involve a large number of files that are heterogeneous and geographically dispersed. Grids are constructed with middleware and software libraries, and the grid computers are connected to a network (i.e., private, public, or the Internet) with a conventional network interface, such as Ethernet. Grid computing does not represent a single point of failure.

### Utility computing means allowing functional users (end-users) to access technology-based services to perform specific and simple tasks (e.g., to run a storage backup program and a disk file recovery program) without requiring much of the technical knowledge. Utility computing does not represent a single point of failure.

### Quantum computing deals with computers with large word sizes with vast amounts of built-in memory power and amazing speed. Quantum computing does not represent a single point of failure.

### Cyber-threat intelligence effort is the acquisition and analysis of information to identify, track, and predict cyber-capabilities, intentions, and activities that offer courses of actions to enhance decision making. Threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. Threat tactics, techniques, and procedures describe the behavior of a threat actor such as a hacker.

### Threat intelligence reports are generally prose documents that describe tactics, techniques, and procedures; threat actors; types of systems and information being targeted; and other threat-related information that provides greater situational awareness to an organization.

### Investment chain connects all of the actors involved in any investment project. A typical investment chain includes many types of actors, such as companies, banks, suppliers, and development finance institutions. ... Money flows in both directions through the investment chain.

### Hash chain is the successive application of a cryptographic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence.

### Packet filtering firewall is a type of firewall that examines each packet and accepts or rejects it based on the security policy programmed into it in the form of traffic rules. This firewall specifies which types of traffic should be permitted or denied and how permitted traffic should be protected, if at all. The packet filtering firewall is not as secure as the screened subnet firewall.

### Screened subnet firewall adds an extra layer of security by creating a network where the bastion host resides. Often called a perimeter network, the screened subnet firewall separates the internal network from the external network. Acting as a perimeter network, if there is an attack on the firewall, the attacker is restricted to the perimeter (external) network and therefore is not attacking the internal network. This leads to a stronger security. Conceptually, the screened subnet firewall is similar to a dual-homed gateway firewall, except that an entire network, rather than a single host, is reachable from the outside. It can be used to locate each component of the firewall on a separate system, thereby increasing throughput and flexibility.

### Screened host firewall combines a packet-filtering router with an application gateway located on the protected subnet side of the router. The screened host firewall is not as secure as the screened subnet firewall.

### Dual-homed gateway firewall is a firewall consisting of a bastion host with two network interfaces, one of which is connected to the protected network, the other of which is connected to the Internet. Internet Protocol (IP) traffic forwarding is usually disabled, restricting all traffic between the two networks to whatever passes through some kind of application proxy. The dual-homed gateway firewall is not as secure as the screened subnet firewall.

### Goal-seeking analysis. “What-if” questions can be applied to goal-seeking analysis. Examples of goal-seeking include introducing a new product or service; entering into a new market; increasing revenue, profits, and market share; and decreasing product and service costs and operating expenses. This means that goal-seeking analysis produces dynamic answers that will change for each type of what-if question. Goal seeking is the process of finding the correct input value when only the output is known.

### What if analysis is the process of changing values in (Microsoft Excel) cells to see how these changes will affect formula outcomes on the worksheet. When you are goal seeking, you are performing a what if analysis on a given value, or the output.

### Situation analysis deals with identifying strengths, weaknesses, opportunities, and threats (SWOT) conditions both internal and external to an organization. SWOT analysis gets information by scanning the internal and external environments of a company. “What-if” questions have nothing to do with the situation analysis because the analysis provides static answers as opposed to dynamic answers.

### Sensitivity analysis determines how different values of an independent variable affect a particular dependent variable under a given set of assumptions. In other words, sensitivity analyses study how various sources of uncertainty in a mathematical model contribute to the model's overall uncertainty. This technique is used within specific boundaries that depend on one or more input variables.

**Question 1: Major risks in issuing an initial coin offering (ICO) for bitcoins?**

1. **Lack of Cyber Security**: BTC is the decentralized peer to peer transaction. Crypto-coins are transported from and to an electronic wallet. The transaction is not backed by any regulatory agency and couldn’t be followed.
2. **Lack of Regulations in Bitcoin Market:** This offers scope for criminal activities, including tax-evasion and money-laundering.
3. **Speculative Bubble:** A speculative bubble is said to be a hike in asset value based upon the exaggerated expectation of future development, appreciation, prices or any other future event that could cause asset valued to pass upward. Bitcoin is a dangerous speculative bubble. Like all bubbles, they burst. They go down, and the one who’s made the last investment gets hurt the most, there’s no question about it.
4. **Price Volatility**
5. **China’s capital outflow**
6. **CMA Test bank: All:-**
7. No central bank to trace money flows
8. No third-party custodian holding the virtual currency
9. No central authority for collecting user information
10. No easy access to third-party business partners

### Question: Fundamental tenet of the defense-in-depth strategy?

A fundamental tenet of the defense-in-depth strategy is to prevent a cyberattack from penetrating networks and to detect and respond effectively to mitigate the effects of attacks that do. Detect-and-respond capabilities are complex structures that run the gamut of intrusion and attack detection, characterization, and response.

Defense in depth is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of information systems. It is an approach for establishing an adequate information assurance (IA) posture whereby

 (1) IA solutions integrate people, technology, and operations;

(2) IA solutions are layered within and among IT assets; and

(3) IA solutions are selected based on their relative level of robustness.

 Implementation of this approach recognizes that the highly interactive nature of information systems and enclaves creates a shared risk environment; therefore, the adequate assurance of any single asset is dependent on the adequate assurance of all interconnecting assets. It is an information protection strategy dealing with controls placed at multiple levels and at multiple places in a given system. It supports agile defense strategy and is the same as security in depth. Defense in depth is a security control.

Question: Trusted Service category?

1. Security
2. Availability
3. Processing Integrity
4. Confidentiality
5. Privacy