C. Trademark laws
D. Copyright laws

Answer: B
Explanation:
Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time. Answer: D is incorrect. Copyright laws protect original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

QUESTION 86
Which of the following types of signatures is used in an Intrusion Detection System to trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash?

A. Access
B. Benign
C. DoS
D. Reconnaissance

Answer: C
Explanation:
Following are the basic categories of signatures: Informational (benign): These types of signatures trigger on normal network activity. For example: ICMP echo requests The opening or closing of TCP or UDP connections Reconnaissance: These types of signatures trigger on attacks that uncover resources and hosts that are reachable, as well as any possible vulnerabilities that they might contain. For example: Reconnaissance attacks include ping sweeps DNS queries Port scanning Access: These types of signatures trigger on access attacks, which include unauthorized access, unauthorized escalation of privileges, and access to protected or sensitive data. For example:

Back Orifice A Unicode attack against the Microsoft IIS NetBus DoS: These types of signatures trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash. For example: TCP SYN floods The Ping of Death Smurf Fraggle Trinoo Tribe Flood Network
QUESTION 87
Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Copyright
B. Snooping
C. Utility model
D. Patent

Answer: D
Explanation:
A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. Answer: A is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer: B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing.

Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage. Answer: C is incorrect. A utility model is an intellectual property right to protect inventions.

QUESTION 88
Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.

A. It creates an alert.
B. It quarantines the file to a secure location.
C. It reconstructs the session.
D. It blocks the transmission of content.

Answer: ABD
Explanation:
When an agent detects a policy violation for data of all states, the Data Loss prevention (DLP) technology takes one of the following actions: It creates an alert. It notifies an administrator of a violation. It quarantines the file to a secure location. It encrypts the file. It blocks the transmission of content. Answer: C is incorrect. Data Loss Prevention (DLP) reconstructs the session when data is in motion.

QUESTION 89
In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?

A. Risk Management
B. Exception management
C. Configuration Management
D. Change Management

Answer: B
Explanation:
Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed data, infrastructure or connectivity issues. It increases the efficiency of business processes and contributes in the progress of business. Answer: C is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process. Answer: A is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager. Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises", so at IT Process Maps we decided to assign clear responsibilities for managing risks. Answer: D is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that

results in a new status of one or more configuration items (CI's)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of Change Management are as follows: Minimal disruption of services Reduction in back-out activities Economic utilization of resources involved in the change

QUESTION 90
Which of the following rated systems of the Orange book has mandatory protection of the TCB?

A. A-rated
B. B-rated
C. D-rated
D. C-rated

Answer: B
Explanation:
A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB).

Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

QUESTION 91
Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?

A. DAS
B. IPsec
C. IDS
D. ACL

Answer: C
Explanation:
An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). Answer: D is incorrect. Access Control List (ACL) is the most commonly used object in Cisco IOS. It filters packets or network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. According to the criteria specified within the access lists, router determines whether the packets to be forwarded or dropped. Access control list criteria could be the source or destination address of the traffic or other information. The types of Cisco ACLs are Standard IP, Extended IP, IPX, Appletalk, etc. Answer: B is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver. Answer: A is incorrect. Direct-attached storage (DAS) is a digital storage system that is directly attached to a server or workstation, without using a storage network.

QUESTION 92
Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

A. Confidentiality
B. OS fingerprinting
C. Reconnaissance
D. Non-repudiation

Answer: D
Explanation:
Non-repudiation is a term that refers to the ability to ensure that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures. Answer: A is incorrect. Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it. Answer: C is incorrect. Reconnaissance is a term that refers to information gathering behaviors that aim to profile the organization, employees, network, and systems before an attack is performed efficiently. It is the first step in the process of intrusion and involves unauthorized discovery and mapping of systems, services, or vulnerabilities. These discovery and mapping techniques are commonly known as scanning and enumeration. Common tools, commands, and utilities used for scanning and enumeration include ping, telnet, nslookup, rpcinfo, File Explorer, finger, etc. Reconnaissance activities take place before performing a malicious attack. These activities are used to increase the probability of successful operation against the target, and to increase the probability of hiding the attacker's identity. Answer: B is incorrect. OS fingerprinting is a process in which an external host sends special traffic on the external network interface of a computer to determine the computer's operating system. It is one of the primary steps taken by hackers in preparing an attack.

QUESTION 93
Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.

A. HTML
B. PHP
C. .NET
D. Perl

Answer: BCD
Explanation:
Perl, .NET, and PHP are examples of the application programming interface (API). API is a set of routines, protocols, and tools that users can use to work with a component, application, or operating system. It consists of one or more DLLs that provide specific functionality. API helps in reducing the development time of applications by reducing application code. Most operating environments, such as MS-Windows, provide an API so that programmers can write applications consistent with the operating environment. Answer: A is incorrect. HTML stands for Hypertext Markup Language. It is a set of markup symbols or codes used to create Web pages and define formatting specifications. The markup tells the Web browser how to display the content of the Web page.

QUESTION 94
In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

A. Chosen plaintext attack
B. Chosen ciphertext attack
C. Ciphertext only attack
D. Known plaintext attack

Answer: C
Explanation:
In a ciphertext only attack, an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

QUESTION 95
The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA? Each correct answer represents a complete solution. Choose all that apply.

A. IATT
B. IATO
C. DATO
D. ATO
E. ATT

Answer: ABCD
Explanation:
The DAA issues one of the following four accreditation determinations: Approval to Operate (ATO): It is an authorization of a DoD information system to process, store, or transmit information. Interim Approval to Operate (IATO): It is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls. Interim Approval to Test (IATT): It is a temporary approval to conduct system testing based on an assessment of the implementation status of the assigned IA Controls. Denial of Approval to Operate (DATO): It is a determination that a DoD information system cannot operate because of an inadequate IA design or failure to implement assigned IA Controls. Answer: E is incorrect. No such type of accreditation determination exists.

QUESTION 96
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Continuity of Operations Plan
B. Contingency Plan
C. Disaster Recovery Plan
D. Business Continuity Plan

Answer: D
Explanation:
BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization