98-367 Q&As

Security Fundamentals

Pass Microsoft 98-367 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

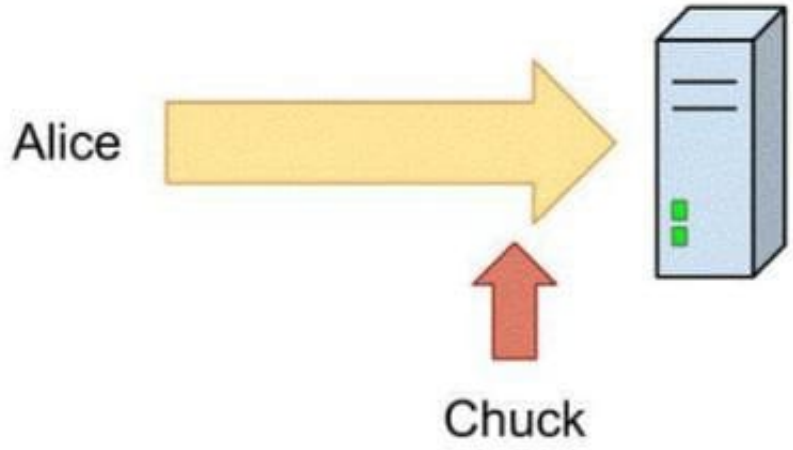
https://www.passapply.com/98-367.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Alice sends her password to the game server in plaintext. Chuck is able to observe her password as shown in the following image:



Use the drop-down menus to select the answer choice that completes each statement. Each correct selection is worth one point.

Hot Area:

Answer Area

The scenario demonstrated is a(n) **[answer choice]** attack.

- man in the middle
- eavesdropping
- denial of service

Alice should **[answer choice]** to avoid this type of attack.

- never send a plaintext password
- only send passwords in plaintext to well-known companies
- only send passwords in plaintext over the local network

Correct Answer:

Answer Area

The scenario demonstrated is a(n) **[answer choice]** attack.

- man in the middle
- eavesdropping
- denial of service

Alice should **[answer choice]** to avoid this type of attack.

- never send a plaintext password
- only send passwords in plaintext to well-known companies
- only send passwords in plaintext over the local network

QUESTION 2

Which of the following types of attack is used to configure a computer to behave as another computer on a trusted network by using the IP address or the physical address?

A. Distributed denial of service (DDOS) attack

B. Honeypot

C. RIP/SAP Spoofing

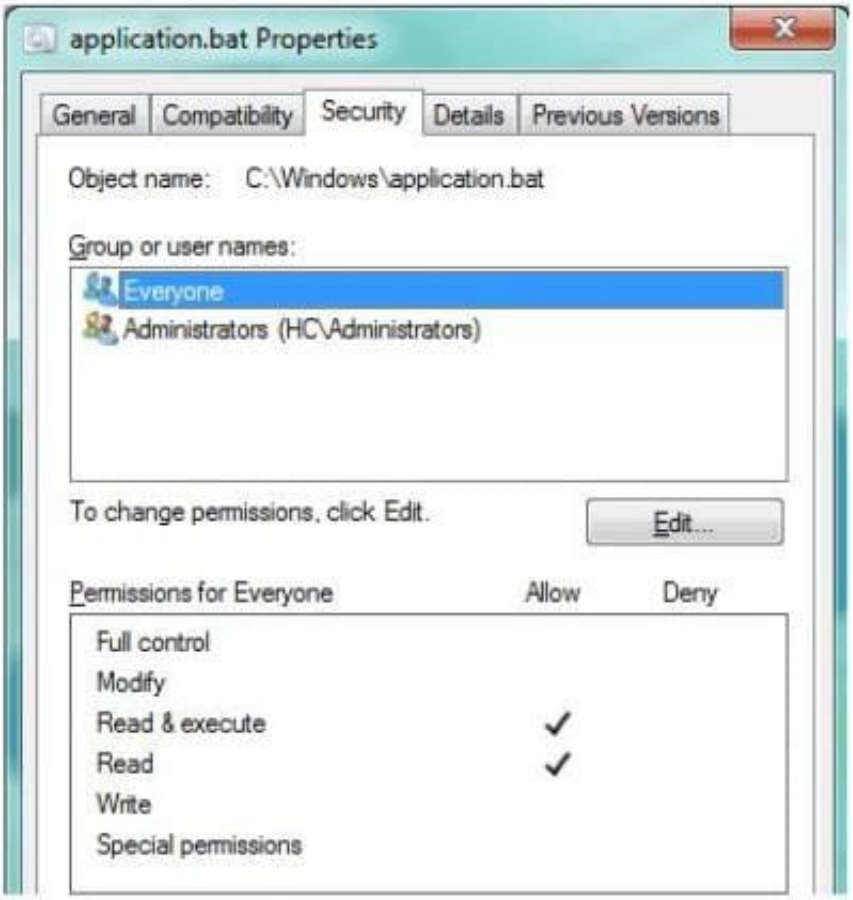
D. Identity spoofing

Correct Answer: D

Identity spoofing (IP address spoofing) will occur when the attacker wants to use an IP address of a network, computer, or network component without being authorized for this task. It allows the unprivileged code to use someone else\\'s identity, and use their security credentials Answer: B is incorrect. A honey pot is a computer that is used to attract potential intruders or attackers. It is for this reason that a honey pot has low security permissions. A honey pot is used to gain information about the intruders and their attack strategies. Answer: C is incorrect. RIP and SAP are used to broadcast network information in a regular way regardless of no changes in the routing or service tables. RIP/SAP spoofing method is used to intercept the SAP and RIP broadcasts by using a spoofing modem/router, and then re-broadcast network information via its own routing table or service table. Answer: A is incorrect. In the distributed denial of service (DDOS) attack, an attacker uses multiple computers throughout the network that it has previously infected. Such computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. TFN, TRIN00, etc. are tools used for the DDoS attack.

QUESTION 3

Your supervisor asks you to review file permission settings on the application.bat file. You need to report which file system the file is on and the type of permission the file has. You review the application Properties dialog box shown in the following image:



Use the drop-down menus to select the answer choice that completes each statement. Each correct selection is worth one point.

Hot Area:

Answer Area

The "cygwin.bat" file in the image is currently on the **[answer choice]** file system.

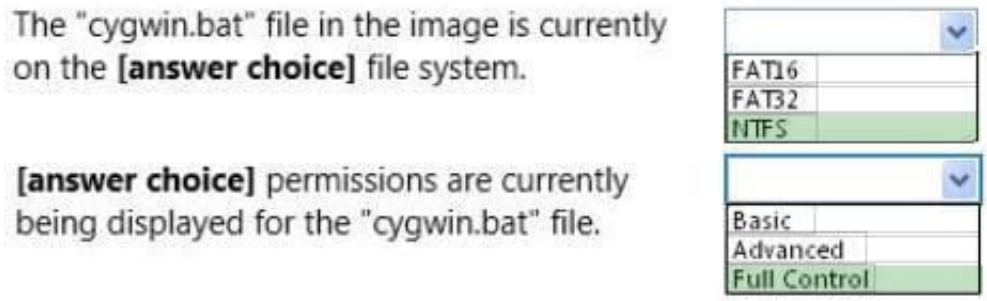
FAT16
FAT32
NTFS

[answer choice] permissions are currently being displayed for the "cygwin.bat" file.

Basic
Advanced
Full Control

Correct Answer:

Answer Area



QUESTION 4

Passwords that contain recognizable words are vulnerable to a:

A. Denial of Service attack

B. Hashing attack

C. Dictionary attack

D. Replay attack

Correct Answer: C

A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

Dictionary attacks work because many computer users and businesses insist on using ordinary words as passwords. Dictionary attacks are rarely successful against systems that employ multiple-word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals. Reference: http://searchsecurity.techtarget.com/definition/dictionary-attack

QUESTION 5

You are a network administrator.

All computers run the Microsoft Edge browser.

You need to prevent web cookies from being saved.

What should you enforce?

A. SmartScreen Filter

B. InPrivate Browsing

C. Antivirus protection

D. Cross-Site Scripting Filter

Correct Answer: B

QUESTION 6

Humongous Insurance is an online healthcare insurance company. During an annual security audit a security firm tests the strength of the company\\'s password policy and suggests that Humongous Insurance implement password history policy.

What is the likely reason that the security firm suggests this?

A. Past passwords were easily cracked by the brute force method.

B. Past passwords of users contained dictionary words.

C. Previous password breaches involved use of past passwords.

D. Past passwords lacked complexity and special characters.

Correct Answer: B

QUESTION 7

Mark works as a Network Administrator fot Blue Well Inc. The company has a Windows-based network. Mark is facing a series of problems with email spam and identifying theft via phishing scams. He wants to implement the various security measures and to provide some education because it is related to the best practices while using email. Which of the following will Mark ask to employees of his company to do when they receive an email from a company they know with a request to click the link to "verify their account information"?

A. Provide the required information

B. Hide the email

C. Use Read-only Domain Controller

D. Delete the email

Correct Answer: D

In the above scenario, Mark will ask his employees to delete the email whenever he receives an email from a company that they know with to click the link to "verify their account information", because companies do not ask for account

information via email now a days.

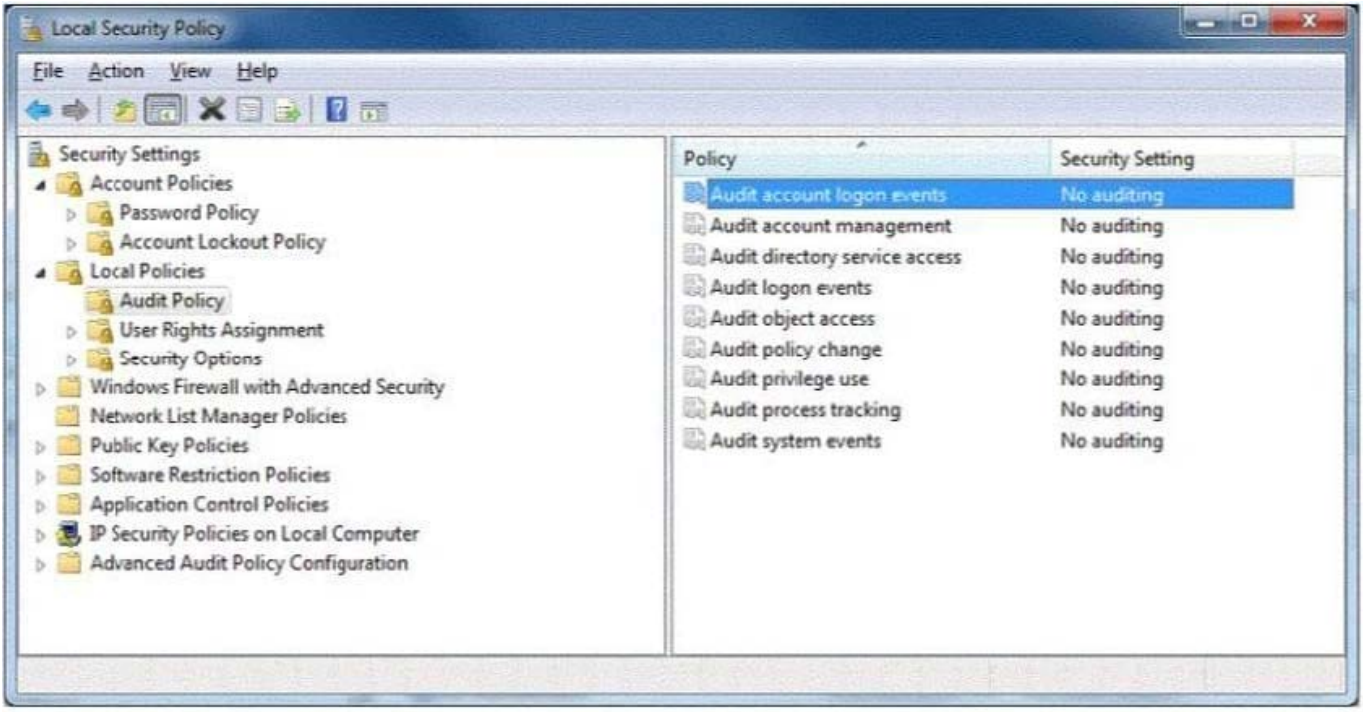
Answer: C is incorrect. Read-only Domain Controller (RODC) is a domain controller that hosts the read-only partition of the Active Directory database. RODC was developed by Microsoft typically to be deployed in a branch office environment.

RODC is a good option to enhance security by placing it in a location where physical security is poor. RODC can also be placed at locations having relatively few users and a poor network bandwidth to the main site. As only the read-only

partition of the Active Directory database is hosted by RODC, a little local IT knowledge is required to maintain it.

QUESTION 8

You are preparing a local audit policy for your workstation. No auditing is enabled. The settings of your policy are shown in the following image:



Use the drop-down menus to select the answer choice that completes each statement. Each correct selection is worth one point.

Hot Area:

Answer Area

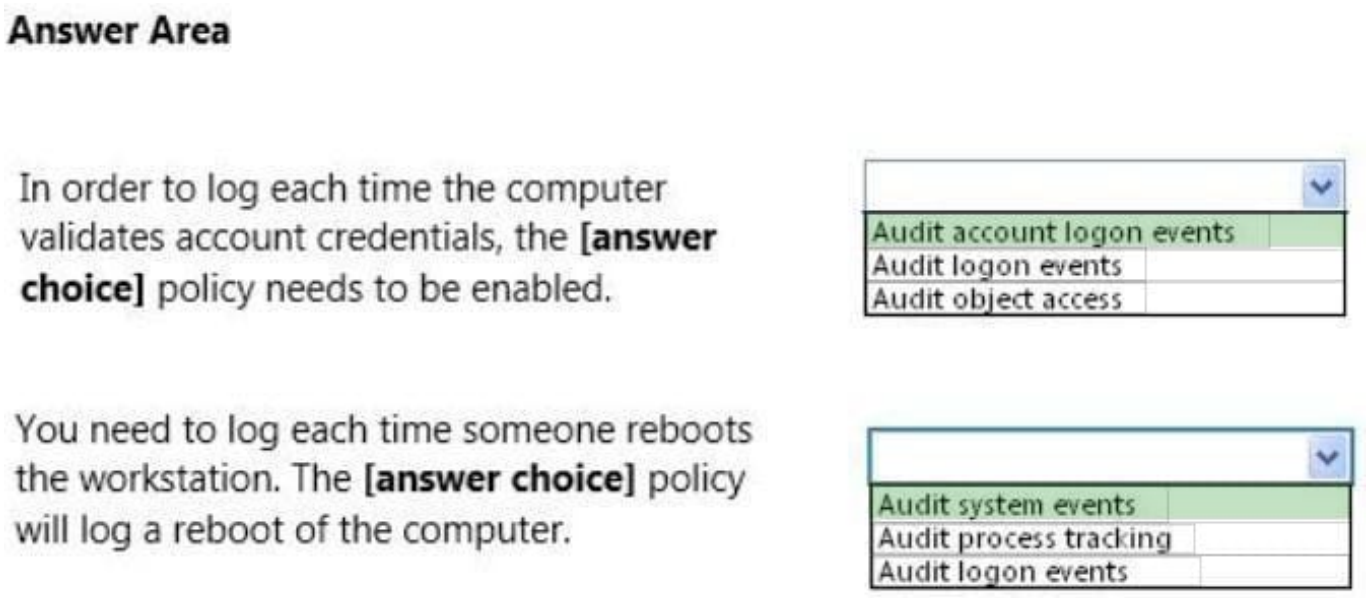
In order to log each time the computer validates account credentials, the **[answer choice]** policy needs to be enabled.

- Audit account logon events
- Audit logon events
- Audit object access

You need to log each time someone reboots the workstation. The **[answer choice]** policy will log a reboot of the computer.

- Audit system events
- Audit process tracking
- Audit logon events

Correct Answer:



Dozens of events can be audited in Windows. The events fall into several categories: Audit account logon events - audit each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. This event category is applicable to domain controllers only since DC\\'s are used to validate accounts in domains.

Audit account management - audit each event of account management on a computer. Examples of account maintenance include password changes, user account and group modifications.

Audit directory service access - audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified.

Audit logon events - audit each instance of a user logging on to or logging off from a computer. Note that this is different than the udit account login events

QUESTION 9

Your Web server crashes at exactly the point where it reaches 1 million total visits. You discover the cause of the server crash is malicious code. Which description best fits this code?

A. Virus

B. Worm

C. Polymorphic Virus

D. Logic Bomb

Correct Answer: D

A logic bomb is malware that executes its malicious activity when a certain condition is met, often when a certain date/time is reached. In this case it waited for the Web server to pass a certain threshold.

QUESTION 10

Which of the following MMC snap-in consoles is used to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest?

A. Active Directory Domains and Trusts

B. Active Directory Administrative Center

C. Group Policy Management Console

D. Active Directory Sites and Services

Correct Answer: D

The Active Directory Sites and Services MMC snap-in console is used to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest.

Answer: A is incorrect. The Active Directory Domains and Trusts console is used to administer domain trusts, domain and forest functional levels, and user principal name (UPN) suffixes.

Answer: B is incorrect. Active Directory Administrative Center is used to administer and publish information in the directory, including managing users, groups, computers, etc.

Answer: C is incorrect. Group Policy Management Console (GPMC) is used to provide a single administrative tool for managing Group Policy across the enterprise.

QUESTION 11

Which of the following is a technique used to attack an Ethernet wired or wireless network?

A. ARP poisoning

B. DNS poisoning

C. Mail bombing

D. Keystroke logging

Correct Answer: A

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The attack can only be used on networks that actually make use of ARP and not another method of address resolution. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. Generally, the aim is to associate the attacker\\'s MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it. ARP spoofing attacks can be run from a compromised host, or from an attacker\\'s machine that is connected directly to the target Ethernet segment. Answer: C is incorrect. Mail bombing is an attack that is used to overwhelm mail servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient\\'s hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack. Answer: B is incorrect. DNS poisoning is the process in which a DNS server may return an incorrect IP address, diverting traffic to another computer. Answer: D is incorrect. Keystroke

logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his keyboard, such as to measure employee\\'s productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc.

QUESTION 12

Which of the following is a set of rules that control the working environment of user accounts and computer accounts?

A. Mandatory Access Control

B. Access control list

C. Group Policy

D. Intrusion detection system

Correct Answer: C

Group Policy is a feature of the Microsoft Windows NT family of operating systems. It is a set of rules, which control the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users\\' settings in an Active Directory environment. Group Policy is often used to restrict certain actions that may pose potential security risks. For example, block access to the Task Manager, restrict access to certain folders, disable the downloading of executable files, and so on. As part of Microsoft\\'s IntelliMirror technologies, Group Policy aims to reduce the cost of supporting users. IntelliMirror technologies relate to the management of disconnected machines or roaming users and include roaming user profiles, folde redirection, and offline files.

Answer: A is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission. Answer: D is incorrect. An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can compromise the security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins, and access to sensitive data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has three main components: Sensors, Console, and Engine. Sensors generate security events. A console is used to alert and control sensors and to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS implementations, these three components are combined into a single device. Basically, the following two types of IDS are used: Network-based IDS Host-based IDS Answer: B is incorrect. Access control list (ACL) is a rule list containing access control entries. It is used to allow or deny access to network resources. ACL can be implemented on network users and network devices such as routers and firewalls. Routers and firewalls use ACL to determine which packets should be forwarded or dropped.

QUESTION 13

Which of the following describes a VLAN?

A. It connects multiple networks and routes data packets.

B. It is a logical broadcast domain across physical subnets.

C. It is a subnetwork that reveals a company\\'s externally facing resources to the public network.

D. It allows different network protocols to communicate between different network segments.

Correct Answer: B

VLAN (Virtual Local Network) is a logically separate IP subnetwork which allow multiple IP networks and subnets to exist on the same-switched network. VLAN is a logical broadcast domain that can span multiple physical LAN segments. It is a modern way administrators configure switches into virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones.

QUESTION 14

Which of the following statements about Network Address Translation (NAT) are true? Each correct answer represents a complete solution. Choose two.

A. It allows the computers in a private network to share a global, ISP assigned address to connect to the Internet.

B. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Host.

C. It allows external network clients access to internal services.

D. It reduces the need for globally unique IP addresses.

Correct Answer: AD

Answer: A and D Network address translation (NAT) is a technique that allows multiple computers to share one or more IP addresses. NAT is configured at the server between a private network and the Internet. It allows the computers in a

private network to share a global, ISP assigned address. It reduces the need for globally unique IP addresses. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from public to private. Answer: B is incorrect. Screened host provides added security by using Internet access to deny or permit certain traffic from the Bastion Host. Answer: C is incorrect. Bastion host allows external network clients access to internal services.

QUESTION 15

You work as a Network Administrator for TechMart Inc. The company has a Windows-based network. After completing a security audit of the company\\'s Microsoft Windows Server 2008 R2 file servers, you have determined that folder and share security requires a revision on the basis of corporate reorganization. You have noticed that some shares on the file system are not secured. Which of the following is a feature that you will use to reassign permissions without assigning permissions to every parent and child folder?

A. Inheritance

B. Kerberos

C. TCP/IP protocol

D. User Account Control (UAC)

Correct Answer: A

Inheritance is defined as the concept of permissions that are propagated to an object from a parent object. It is found in both file system permissions and Active Directory permissions and does not work with share permissions. It is used to reassign permissions without assigning permissions to every parent and child folder Answer: B is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: D is incorrect. User Account Control (UAC) is used to prevent unauthorized changes to computers on the domain. Answer: C is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for communicating with each other over the internet.