

Final Exam



Sourav Mangla (username: souravmangla)

Attempt 1

Written: May 2, 2023 11:09 AM - May 2, 2023 12:03 PM

Submission View

Your quiz has been submitted successfully.

Question 1

2 / 2 points

The Post Office Protocol version 3 uses TCP port 110.

- ✓ ☐ 1) True
☐ 2) False

Question 2

2 / 2 points

It is important to understand the underlying impact of potential disasters for business continuity and contingency planning.

- ✓ ☐ 1) True
☐ 2) False

Question 3

2 / 2 points

Spoofing is a technique in which the address of the source is changed to make a packet appear as if it was coming from a legitimate source.

- ✓ ☐ 1) True
☐ 2) False

Question 4

2 / 2 points

Internet Explorer is currently the most popular web browser worldwide.

- ☐ 1) True
✓ ☐ 2) False

Question 5

2 / 2 points

Data warehouses should be stored on the same server as the main transactional database.

- ☐ 1) True
✓ ☐ 2) False

Question 6

0 / 2 points

It is not necessary to ensure that basic Internet protocols are kept secure.

- ✗ ☐ 1) True
➡ ☐ 2) False

Question 7

2 / 2 points

A Class B IP Address is used in medium sized networks, such as the University of Arizona.

- ✓ ☐ 1) True
- ☐ 2) False

Question 8**2 / 2 points**

During a Business Impact Analysis, no consideration should be given to how quickly systems must be brought back online.

- ☐ 1) True
- ✓ ☐ 2) False

Question 9**2 / 2 points**

IMAP uses UDP port 143.

- ☐ 1) True
- ✓ ☐ 2) False

Question 10**2 / 2 points**

Software RAID is implemented through the Operating System.

- ✓ ☐ 1) True
- ☐ 2) False

Question 11**2 / 2 points**

An e-mail address contains both a local address and a host address separated by an @ symbol.

- ✓ ☐ 1) True
- ☐ 2) False

Question 12**2 / 2 points**

One type of UPS system is called an Online UPS.

- ✓ ☐ 1) True
- ☐ 2) False

Question 13**2 / 2 points**

The 802.11 wireless standard focuses on the use of the physical and data-link layers of the OSI model.

- ✓ ☐ 1) True
- ☐ 2) False

Question 14**2 / 2 points**

A rogue access point with a long-range antenna makes it possible to monitor a network from a greater distance without being observed.

- ✓ ☐ 1) True
- ☐ 2) False

Question 15**2 / 2 points**

RAID level 6 stripes data across at least 3 hard drives, spreading parity data across all drives for redundancy.

- ✓ ☐ 1) True
☐ 2) False

Question 16**2 / 2 points**

Cache poisoning is an attack caused by the direct use of command-line e-mail tools.

- ☐ 1) True
✓ ☐ 2) False

Question 17**2 / 2 points**

The bluetooth wireless standard uses frequency hopping in the 2.4 GHz band.

- ✓ ☐ 1) True
☐ 2) False

Question 18**0 / 2 points**

HTTP operates over TCP port 443.

- ✗ ☐ 1) True
➡ ☐ 2) False

Question 19**2 / 2 points**

Secure Hypertext Transfer Protocol (S-HTTP) is the only secure form of the HTTP protocol.

- ☐ 1) True
✓ ☐ 2) False

Question 20**2 / 2 points**

A virtual private network acts like a tunnel through a larger network.

- ✓ ☐ 1) True
☐ 2) False

Question 21**2 / 2 points**

In Canada and the United States, the 802.11b wireless networking standard uses _____ possible channels.

- ☐ 4
☐ 10
✓ ☐ 11
☐ 13

Question 22**2 / 2 points**

Which of the following statements about uninterruptable power supplies is false?

- ☐ A UPS is the best fault-tolerance method to prevent power problems.
- ☐ A UPS allows users to save data and safely shut down systems during a power failure.
- ✓ ☒ A UPS is only built into electrical equipment.
- ☐ A UPS provides immediate battery power during a brownout or power failure.

Question 23**2 / 2 points**

Which encryption method is used in PGP?

- ☐ CAST
- ☐ IDEA
- ☐ 3DES
- ☐ Both A and B
- ✓ ☒ A, B, and C

Question 24**2 / 2 points**

The NetBIOS Extended User Interface (NetBEUI) protocol is used by which operating system(s).

- ✓ ☒ Windows
- ☐ Linux
- ☐ Mac OS X
- ☐ Novell Netware

Question 25**2 / 2 points**

The Network File System uses remote procedure calls via TCP port _____?

- ☐ 25
- ☐ 80
- ✓ ☒ 111

☐ 443

Question 26**0 / 2 points**

Which statement regarding passive intrusion detections systems is true?

- ☐ A passive IDS includes taking action on findings.
- ➔ ☐ A passive IDS is only effective if the sysadmin regularly checks the logs.
- ☐ A passive IDS can be configured to take action or thwart attacks.
- ✗ ☐ A passive IDS only monitors the specific system it is installed on.

Question 27**2 / 2 points**

Microsoft's Remote Access Services is capable of handling how many simultaneous connections?

- ☐ 1-9
- ☐ 10-20
- ☐ 25-50
- ✓ ☐ 100+

Question 28**2 / 2 points**

This type of packet filtering tracks information about a communication session, such as the ports in use.

- ☐ stateless
- ☐ statemore
- ✓ ☐ stateful
- ☐ statemin

Question 29**2 / 2 points**

Which connection types are supported by RAS?

- ☐ ISDN
- ☐ DSL
- ☐ Frame Relay

✓ ☐ All of the Above

Question 30**2 / 2 points**

Microsoft Internet Explorer enables security configurations through which zones?

- ☐ Internet Zone
- ☐ Local Intranet Zone
- ☐ Trusted Sites
- ✓ ☐ All of the Above

Question 31**2 / 2 points**

Which of the following authentication types is not available for use in a RAS policy?

- ☐ Challenge Handshake Authentication Protocol
- ☐ Extensible Authentication Protocol
- ☐ Unauthenticated
- ✓ ☐ All of the above are available for use in RAS.

Question 32**2 / 2 points**

Which UDP port is used for SMB file sharing?

- ☐ 21
- ☐ 389
- ✓ ☐ 445
- ☐ 1433

Question 33**2 / 2 points**

The recommended NAT IP Address ranges for a Class B network is _____.

- ☐ 10.0.0.0 to 10.255.255.255
- ☐ 127.0.0.0 to 127.255.255.255
- ✓ ☐ 172.16.0.0 to 172.31.255.255

☐ 192.168.0.0 to 192.168.255.255

Question 34**2 / 2 points**

Server Message Block requires which firewall port(s) to be open?

☐ TCP 443

☐ TCP 445

☐ UDP 445

☐ Both A and B

✓ ☒ Both B and C

Question 35**2 / 2 points**

This IP Address class is used for experimentation.

☐ Class A

☐ Class B

☐ Class C

☐ Class D

✓ ☒ Class E

Question 36**2 / 2 points**

Which of the following log types are available in Windows Event Viewer?

☐ Application

☐ Firewall

☐ System

☐ Both A and B

✓ ☒ Both A and C

Question 37**2 / 2 points**

TCP/IP consists of _____ nonproprietary protocols.

- ☐ 75
- ☐ 90
- ✓ ☐ 100
- ☐ 115

Question 38**2 / 2 points**

This IP Address class is composed of up to 16,777,214 stations.

- ✓ ☐ Class A
- ☐ Class B
- ☐ Class C
- ☐ Class D
- ☐ Class E

Question 39**2 / 2 points**

Which remote access protocol was originally designed for UNIX environments?

- ✓ ☐ SLIP
- ☐ PPP
- ☐ L2TP
- ☐ PPTP

Question 40**2 / 2 points**

S/MIME encryption was developed in _____.

- ☐ 1990
- ✓ ☐ 1995
- ☐ 2000
- ☐ 2005

Question 41**0 / 20 points**

You are the system administrator for a healthcare company opening a new office location. This company is responsible for digitizing health records for hospitals and doctor's offices, so the company processes and stores a significant amount of personal information on their information systems. With this understanding, you have been given the responsibility for planning the security design of the network. The company has allocated a total budget of \$30,000.00 for this project. After evaluating the situation, you have created a list of potential options for securing the network, along with the cost associated with adopting each security option (some are more expensive than others). Since you have a limited budget, it will be impossible to choose every option, so you must decide which options are the most important for this company to adopt to remain within the \$30,000.00 budget figure. You will need to make your selections and present them to management. Management is expecting a brief justification for each option you selected and why you feel the selections you made (as viewed together) will be sufficient for securing the network.

Options: Network Firewall (\$10,000), Intrusion Detection System (\$15,000), Intrusion Prevention System (\$25,000), Honeypot (\$2,500), DMZ (\$20,000), Network Monitoring Software (\$5,000), Proxy Server (\$8,000), Anti-Virus Software (\$5,000 - 250 licenses), Network-based Anti-Spam System (\$10,000), Vulnerability Scanning Software (\$12,500).

Responses to this short essay must be a minimum of 300 to 350 words. It is recommended you write this essay in a word processor then copy/paste your response into the answer field.

As a system administrator for a healthcare company, it is important to safeguard the network to prevent unwanted access and attacks. With a budget of \$30,000 it is critical to select the correct security alternatives that will provide the best network protection while remaining in the budget.

A network firewall is a critical security tool that monitors and regulates incoming and outgoing network traffic based on the predefined security rules. It can prevent unauthorized network access, defend against DoS and DDoS attacks and limit access to critical data. A firewall is a must-have security measure to protect against cyber threats.

Another feature is an IDS and its ability to monitor network traffic and detect abnormal activities that could suggest an attack. It can notify the security staff of potential risks, allowing them to investigate and respond to attacks as soon as possible. A IDS is a proactive security option that can prevent data loss or harm from unauthorized access.

Antivirus software is another critical security measure for preventing malware from identifying the network. Viruses, spyware and other unwanted software can be detected and removed using this. It can detect threats in files, emails and web pages and quarantine or remove the affected files. The healthcare organization may safeguard all of its equipments, including desktops and mobile devices, by purchasing 250 licenses of this software.

Together, these security methods will give a solid combination of network protection while remaining within the budget. The network firewall will prevent unauthorized access and defend against DoS and DDoS attacks. The IDS will detect unusual activity and antivirus software will protect against malware. While the other options on the list are beneficial for network security, they are not as critical for the healthcare company's specific needs and budget constraints as the firewall, IDS and antivirus software. The above software costing \$5000, \$15,000 and \$5000 respectively fit within the company's budget of \$30,000 and can help strengthen the company's network security.

This question has not been graded.

The correct answer is not displayed for Written Response type questions.

Attempt Score: 74 / 100 - 74 %**Overall Grade (highest attempt): 74 / 100 - 74 %**

Done