REVIEW PAPER (IDPS)

By: Zeeshan Sajid

MS CS 4th Semester

ID 14289

Abstract: Intrusion detection systems (IDS) is a hardware device or software application, which uses the known intrusion signatures to detect and analyze the inbound and outbound network traffic if there is an abnormality activity. Intrusion prevent system (IPS) supplements the intrusion detection system (IDS) configuration by actively checking the incoming traffic of the system to clear malicious requests. researcher group has been worked an updated review on the use of IDPs to identify vulnerabilities in various channels for accessing data through a network or system and the prevention mechanisms used to mitigate intrusions. In this review we identified that research and development trends seem to be merging into a multi-agent IDPs that is based on and managed by an autonomous computing paradigm, combined with advanced technologies such as natural language processing, artificial intelligence, and data mining to help improve abnormal ID , Based on its self-managed attributes, such as self-configuration, self-optimization, self-healing, and self-protection. These autonomous computing attributes must be expanded to include self-detection and self-prevention.

1. Introduction

Intrusion detection systems (IDS) is a hardware device or software application, which uses the known intrusion signatures to detect and analyze the inbound and outbound network traffic if there is an abnormality activity. Intrusion prevent system (IPS) supplements the intrusion detection system (IDS) configuration by actively checking the incoming traffic of the system to clear malicious requests. Typical IPS configurations use web application firewalls and traffic filtering solutions to protect application security. Therefore, Intrusion detection is a method of observing events in the system and investigating potential events, signs of violations or proximity to security measures. Intrusion prevention is a method of performing intrusion detection and then stopping the identified situation. Intrusion is a criminal demonstration against a data system (for example, a PC system, system, or web framework) that destroys or bargains, leaving the system in an unstable state, thereby allowing unauthorized access. Facilitate system supervision information system. This should be possible by bypassing, weakening, or investigating vulnerabilities on the system. In most cases, intrusion detection systems can find these vulnerabilities. The researcher team has conducted an updated investigation on IDPs utilization to distinguish vulnerabilities in different channels. These vulnerabilities can obtain information through a system as well as prevention components for justifying intrusions [1]. In this review we focusing on background of the existing survey paper.

2. Background

Between 1984 and 1986, several researchers conducted more research on intrusion detection systems. James P. Anderson's paper [2] introduced the research of Intrusion detection framework (IDS). In the mid-1990s, IDS products were first marketed by two organizations, Web Security Framework Inc (ISS) and Wheel-gathering. They planned a system-based IDS called a true security and cyber officer. ISS Inc. released the main form of Genuine Secure 1.0 for Windows NT 4.0. True security uses information bases by coordinating tags, but it is not enough to resist new attacks, which becomes fundamentally difficult. At the time, Wheel-gathering's Net-leger was a system-based IDS, which was completed on time as early as 1995. It works by filtering system traffic.

Wheel-bunch was acquired by Cisco in February 1998. Today, it has become a fundamental part of Cisco security. Many analysts find that they are not satisfied with the use of information-based trademark coordination innovation because it needs to constantly refresh the database to distinguish new attacks. More importantly, system and information bundling transactions began to grow to gigabits at a rate of a few megabits per second. This is an important test because it is increasingly difficult to continuously filter, investigate traffic, and identify attacks. Therefore, scientists need to plan IDS for fast systems. This prompted the creation of host-based IDS, such as TCP Wrappers, Tripwire and Grunt, which can gradually study the framework logo. Grunt is a free IDS device, known for its online flexibility and IDS-based features. It was first released by Marty Roesch1 for the UNIX framework on December 22, 1998. Later in 1999, an adapted version of Grunt (version 1.5) was released. It can successfully investigate and record information packages gradually; later Michael Davis (Michael Davis) changed it for the Windows framework in 2000. [3].

Currently, with the development of IDS capabilities, attackers are now exploring ways to detect, bypass, and disable IDS before infiltrating the infrastructure, leading to a denial of service (DoS). Security experts aim to contain these attacks through the use of intrusion detection and prevention system (IDPs) architectures, which are invisible to attackers. It does this by limiting the communications allowed between several security mechanisms on the network. As the number of vulnerabilities gradually increases, it is important to identify attacks. To this end, there are many reviews of IDPs in [4], the most recent review was in 2016. Since then, many things worth reporting has happened. For example, in 2016, the botnet recorded the largest DDoS attack. One example is Mirai, which is a botnet that is mainly collected of infected routers and security cameras, and low-power less secure devices that have caused many major DDoS attacks .

At this point, society has been embracing data innovation (IT) for a long time. With the development of online business, this is now more important than any other time in recent memory. Individuals rely on PC systems to provide them with news, stock costs, e-mail and online shopping. The details of individual charge cards, clinical records and other personal data are kept in the PC frame. Many organizations consider network proximity as an essential part of their business. The inspection network uses the PC framework to include inspection and decentralized discovery. The PC controls the basic parts of the country, such as the force framework. The respect and accessibility of each of these frameworks must be ensured to prevent dangers. Beginner programmers, competing partnerships, radicals and even external governments have thought processes and capabilities to perform advanced attacks on PC frameworks. Subsequently, in the field of data, more importantly, communication security is critical to the well-being of society and the prosperity of money. In addition, to discover protection vulnerabilities, security requires a breakthrough intrusion detection and Prevention system (IDPs).

In most cases, the organization intrusion detection system is the center. The security components here are inherently easy to use, precise, easy to control, categorize, respectable and ID. Plug-in attacks can be divided into potential attacks and dynamic attacks. This kind of attack is called a functional attack when the information is changed or the entire system is facilitated by the information. Normal operation is an interference. This can include denial of management (DoS), distributed denial of management (DDoS), SQL injection, development, replay attacks, disguise, and changes. A few examples that do not involve attacks include traffic inspection, sniffing, and keyloggers. The disadvantage of this check is that the order of the intrusion detection system is cited, but it does not appear. Similarly, it is recognized that the organization IDPS can distinguish the hub's abnormal behavior only after the damage to the organization's assets.

In existing paper, they completely explained prevention systems and intrusion detection as well as its classification, types, advantages and disadvantages, design and architecture. We exploring all these one by one in background study.

2.1 Intrusion detection and prevention systems

Today, security experts are leaning on security gadgets that add intrusion detection and protection capabilities. These capabilities can identify, log potential events, stop attacks and send reports to supervisors. Intrusion detection and prevention system (IDP) guarantees the security of the data system. While keeping the data system in a safe state, IDP plays an important role in storing information, preventing information from being accidentally authorized to be accessed or robbed, and protecting data. Not long ago, attackers focused on bank customers who attacked their accounts by mistakenly obtaining personal data (by sending phishing messages).

2.2 Classification of IDPs

In this section the authors intrusion detection and prevention systems classified in main three categories.

2.2.1 Type of Intruder

This is outside or inside. Outside gatecrashers don't have any type of access rights to the system or administrations, while interior interlopers are the individuals who have approved access to the system however have restricted rights to the system.

2.2.2 Second types of intrusions.

2.2.3 Third detection technology.

Intrusion detection, abuse detection, non-compliance detection, and status engagement investigations have all used three different innovations to a large extent. In terms of detection innovation, they completely talked about malicious detection, which is a marker-based detection strategy that can coordinate the attack examples and signs of gate attackers and provide a database of known vulnerabilities for programs and system vulnerabilities. Odd number-based detection is a behavior-based detection innovation, and its contribution can be obtained from the inspection log generated by the working system. A state agreement survey is a check that determines changes in agreement conditions. Standards-based procedures include choosing solutions based on many rules characterized by regional experts. They can identify known attacks, but they cannot identify novel attacks. Managed AI (ML) does not need to be displayed like irregular detection. It can learn complex harmful and typical models. The case of AI alone is based on bundle IDP. This intrusion detection strategy includes building models using unlabeled information. In any case, their speech is not in the same class as the well-regulated role model.

2.3 Types of IDPs

2.3.1 Network-Based IDPs

Network-based IDPs (NIDPs) expertise is designed to examine the Open System Interconnection (OSI) model of network, transmission, and application-level data packets. When NIDPS is deployed in a network structure with a precise design, NIDPS is the most efficient. It can monitor and evaluate real-time data packages for intrusion and make decisions about any suspicious activity.

2.3.2 Wireless IDPs

WIDPs is an irregular of NIDPS that can monitor and analyze data packets and protocols on the wireless network. Although WIDPS has the capability to examine network traffic, it cannot Perceive abnormal activity in the software.

2.3.3 Network Behavior Analysis (NBA)

NBA is a variant of NIDPS, with a screening function and decomposition of the flow system to distinguish between abnormal exercise due arrange infringement, DDoS attacks or malware that may be created.

2.3.4 Host-based IDPs

The host-based IDPs innovation plan distinguishes and prevents application-level intrusion and work system intrusion by observing the introduction of a single host into the host. Despite its ability to filter and investigate organizational traffic, HIDPS can still break down explicit system settings, such as program calls, neighbor security policies, and logs used to check suspicious operations on the host.

2.4 Design and Architecture

The current data system has become the target of programmers. The only reason for programmers is to eliminate the respect, accessibility and classification of information. Therefore, when planning an IDPs, appropriate structural considerations must be considered to enhance its ability to identify hazards and prevent them from accessing data systems. In design of intrusion detection and prevention system most important thing is sensitivity of it based on speed and accuracy like, true negative case, false negative case, true positive case and false positive case. It is identifying by precision, recall and average accuracy. In architecture first centralized is using for collecting data from one node or hosts or several hosts. After they send data to single medium for data analysis. The next is hierarchical architecture they collecting information or data from multiple host and performing utilization based on IDPs layers. The last is distributed which is only host to host working for collecting data and analyze.

3. Conclusion

In this paper we briefly identified the background of previous research paper of intrusion detection and prevention system. In existing paper, the authors completely described intrusion detection its software application. They briefly explained classification of intrusion recognition and prevention systems, types of it, design and architecture. They main focused on background of intrusion recognition but they cannot explain about risk of intrusion detection, not explain security for intrusion and not explain artificial intelligent system for intrusion detection. Because they only focused on malicious activity and prevention system. it is important focus on machine learning and artificial intelligence advance technology for intrusion recognition and prevention system to improve intrusion detection and make intelligent application for it. because in machine learning supervised learning is very sufficient for abnormal and normal intrusion classification. While unsupervised learning is more reliable for intrusion detection-based cluster. After that intelligent application is more powerful for real time intrusion detection. So, it is important to focus on this merging area for intrusion detection and prevention system.

Research and development trends seem to be merging into a multi-agent IDPs that is based on and managed by an autonomous computing paradigm, combined with advanced technologies such as natural language processing, artificial intelligence, and data mining to help improve abnormal ID , Based on its self-managed attributes, such as self-configuration, self-optimization, self-healing, and self-protection. These autonomous computing attributes must be expanded to include self-detection and self-prevention. The results of these techniques will help analysts distinguish malicious attack activities from normal daily non-attack activities. They will make IDP intelligent and become a powerful part of the security management system. Through rich and simplified alarm processing and the presentation of security violation activities, it is easy to use.

REFERENCES

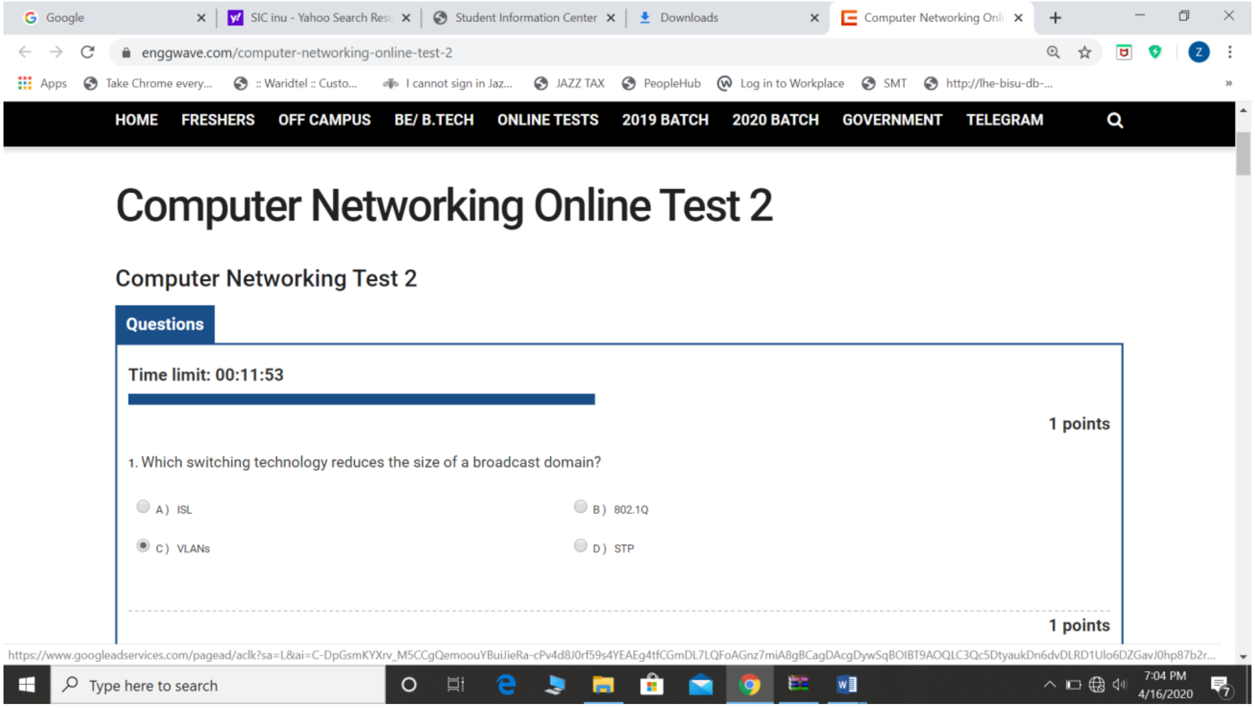
[1] Nureni Ayofe Azeez1, Taiwo Mayowa Bada2, Sanjay Misra3, Adewole Adewumi4, Charles Van der Vyver5 and Ravin Ahuja6 “Intrusion-detection and prevention system-An Updated Review” *SPSS white paper Data Management, Analytics and Innovation, Advances in Intelligent Systems and Computing 1042, https://doi.org/10.1007/978-981-32-9949 -8_48* 2020.

[2] Anderson and J.P2 “Computer Security Planning Study Washington”. Retrieved *fromhttps://pdfs.semanticscholar.org/0735/6c5477c83773bd062b525f45c433e5b044e8.pdf.* 2019.

[3] Bruneau, G “The History and Evolution of Intrusion Detection”. Retrieved from” *https://www.sans.org/reading-room/whitepapers/detection/history-evolution intrusion-detection- 344* 2011.

[4] Patel, 1., Taghavi, M2., Bakhtiyari, K3 and Júnior J.C4 “An intrusion detection and prevention system in cloud computing: A systematic review*”. J. Netw. Comput. Appl. 36, 25–41* 2013.

Screenshots of Quiz


Google
SIC inu - Yahoo Search Resu
Student Information Center
Downloads
Computer Networking Onli
enggwave.com/computer-networking-online-test-2
Apps
Take Chrome every...
:: Waridtel :: Custo...
I cannot sign in Jaz...
JAZZ TAX
PeopleHub
Log in to Workplace
SMT
http://lhe-bisu-db-...
HOME
FRESHERS
OFF CAMPUS
BE/ B.TECH
ONLINE TESTS
2019 BATCH
2020 BATCH
GOVERNMENT
TELEGRAM
https://www.googleadservices.com/pagead/aclk?sa=L&ai=C-DpGsmKYXrv_M5CCgQemoouYBuiJieRa-cPv4d8J0rf59s4YEAEg4tfCGmDL7LQFoAGnz7miA8gBCagDAcgDywSqBOIBT9AOQLC3Qc5DtyaukDn6dvDLRD1Ulo6DZGavJ0hp87b2r...
Type here to search
7:04 PM
4/16/2020

Computer Networking Online Test 2

Computer Networking Test 2

Questions

Time limit: 00:11:53

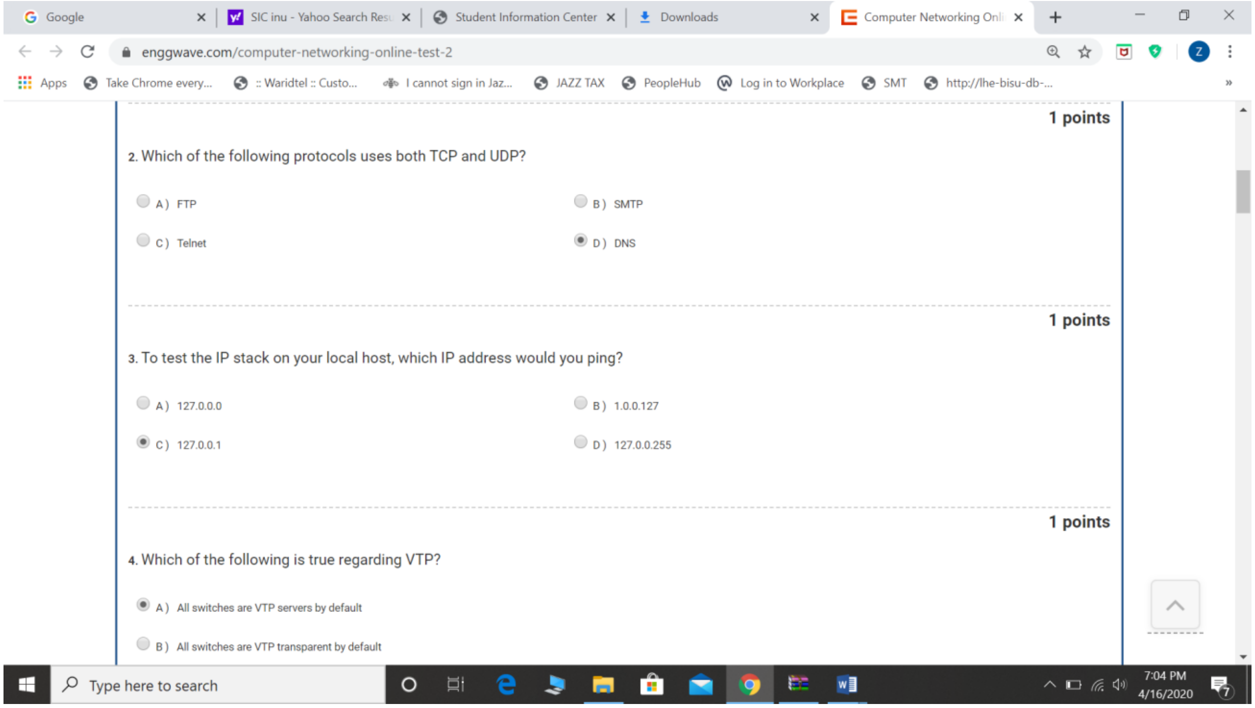
1 points

1. Which switching technology reduces the size of a broadcast domain?

○ A) ISL ○ B) 802.1Q

● C) VLANs ○ D) STP

1 points



1 points

2. Which of the following protocols uses both TCP and UDP?

○ A) FTP ○ B) SMTP

○ C) Telnet ● D) DNS

1 points

3. To test the IP stack on your local host, which IP address would you ping?

○ A) 127.0.0.0 ○ B) 1.0.0.127

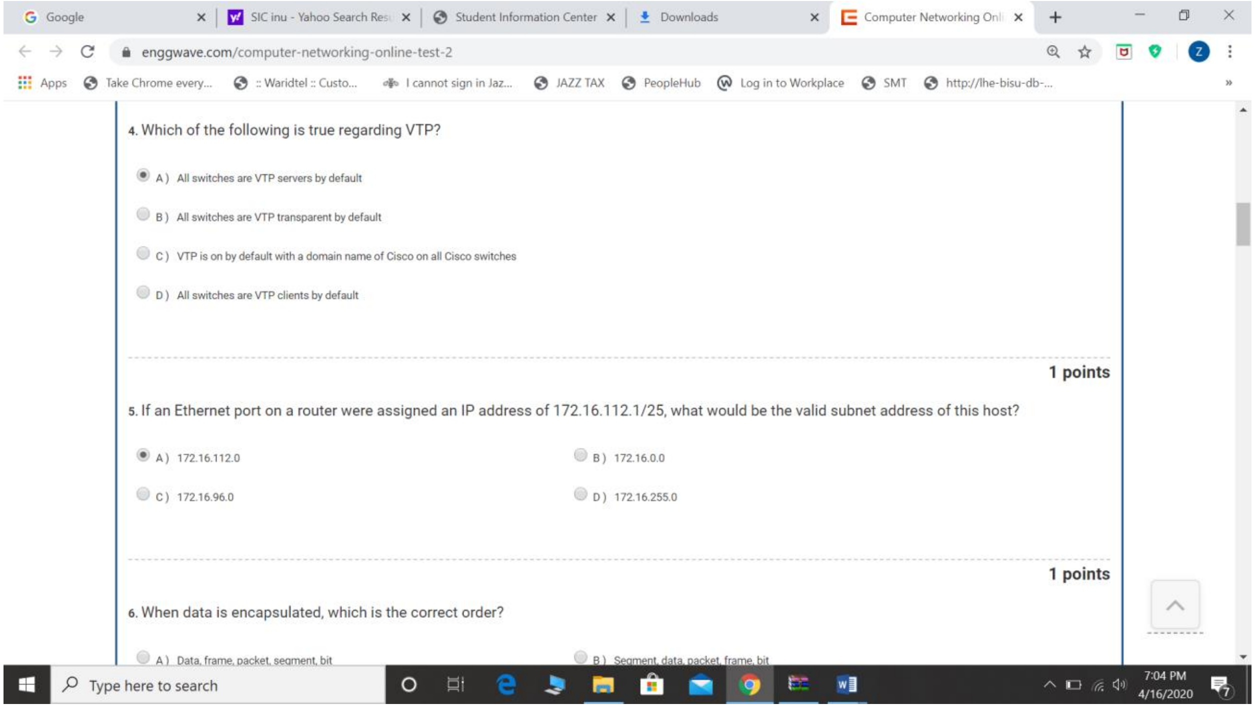
● C) 127.0.0.1 ○ D) 127.0.0.255

1 points

4. Which of the following is true regarding VTP?

● A) All switches are VTP servers by default

○ B) All switches are VTP transparent by default



4. Which of the following is true regarding VTP?

● A) All switches are VTP servers by default

○ B) All switches are VTP transparent by default

○ C) VTP is on by default with a domain name of Cisco on all Cisco switches

○ D) All switches are VTP clients by default

1 points

5. If an Ethernet port on a router were assigned an IP address of 172.16.112.1/25, what would be the valid subnet address of this host?

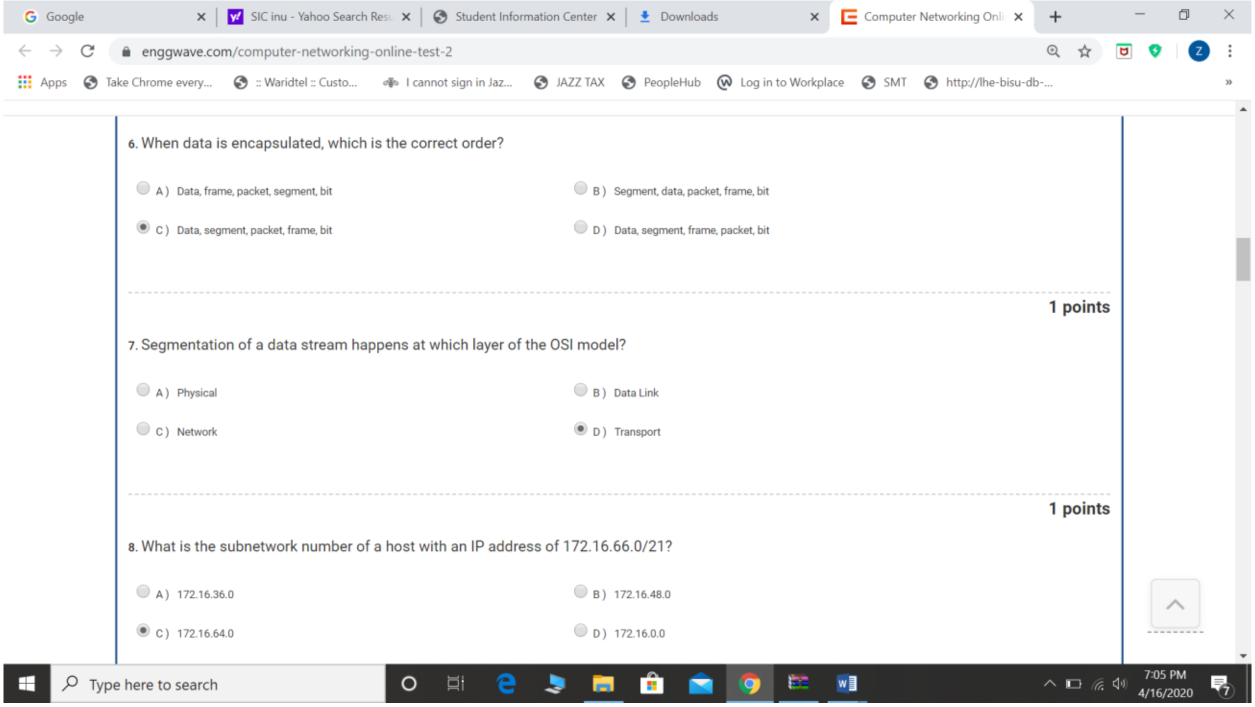
● A) 172.16.112.0 ○ B) 172.16.0.0

○ C) 172.16.96.0 ○ D) 172.16.255.0

1 points

6. When data is encapsulated, which is the correct order?

○ A) Data, frame, packet, segment, bit ○ B) Segment, data, packet, frame, bit



6. When data is encapsulated, which is the correct order?

○ A) Data, frame, packet, segment, bit ○ B) Segment, data, packet, frame, bit

● C) Data, segment, packet, frame, bit ○ D) Data, segment, frame, packet, bit

1 points

7. Segmentation of a data stream happens at which layer of the OSI model?

○ A) Physical ○ B) Data Link

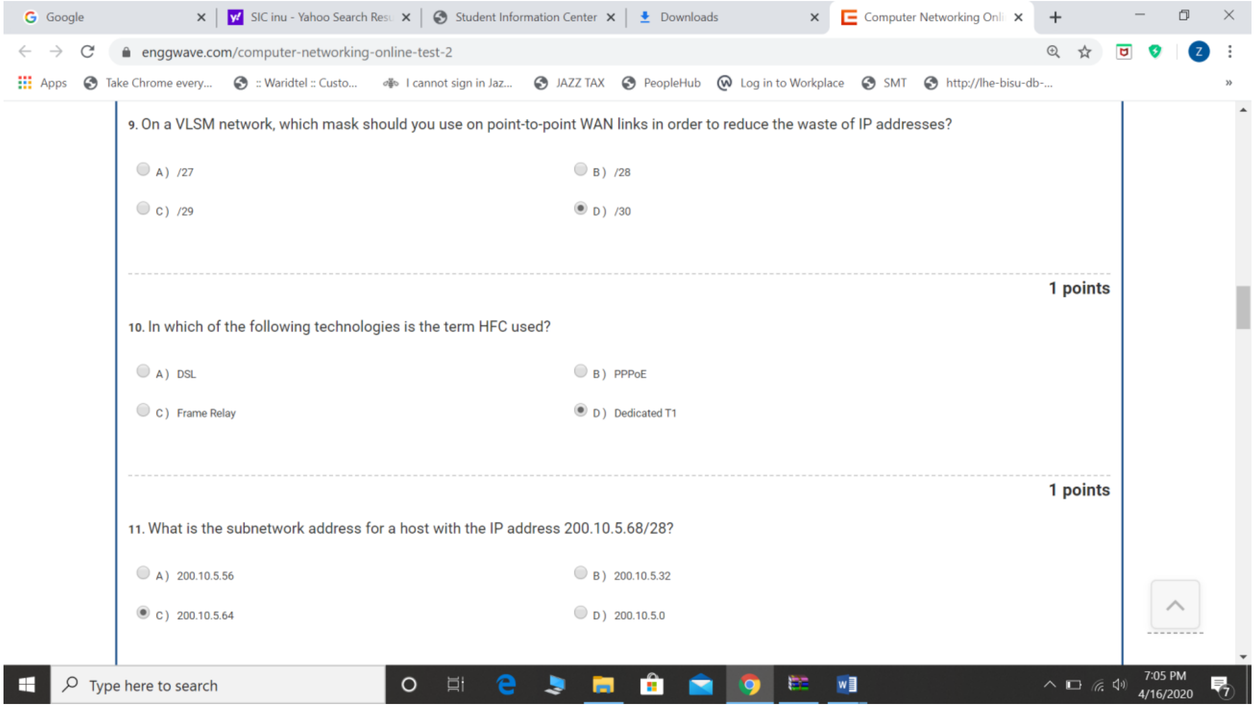
○ C) Network ● D) Transport

1 points

8. What is the subnetwork number of a host with an IP address of 172.16.66.0/21?

○ A) 172.16.36.0 ○ B) 172.16.48.0

● C) 172.16.64.0 ○ D) 172.16.0.0



9. On a VLSM network, which mask should you use on point-to-point WAN links in order to reduce the waste of IP addresses?

○ A) /27 ○ B) /28

○ C) /29 ● D) /30

1 points

10. In which of the following technologies is the term HFC used?

○ A) DSL ○ B) PPPoE

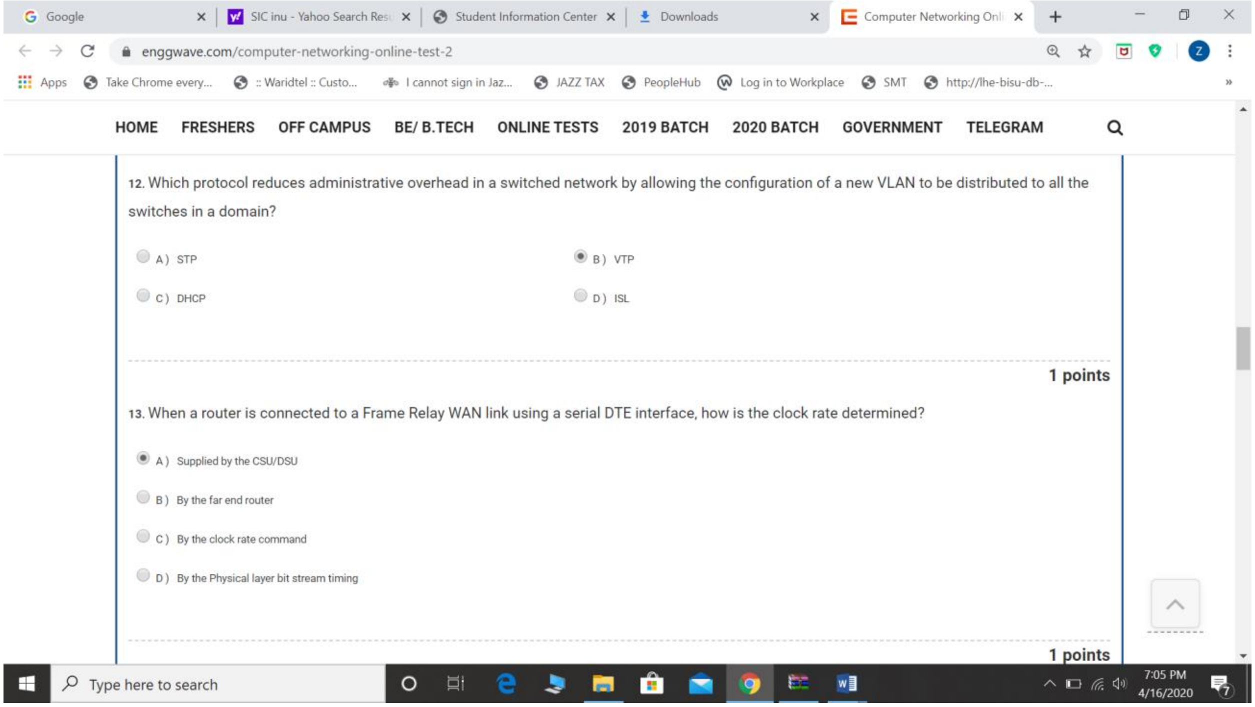
○ C) Frame Relay ● D) Dedicated T1

1 points

11. What is the subnetwork address for a host with the IP address 200.10.5.68/28?

○ A) 200.10.5.56 ○ B) 200.10.5.32

● C) 200.10.5.64 ○ D) 200.10.5.0



12. Which protocol reduces administrative overhead in a switched network by allowing the configuration of a new VLAN to be distributed to all the switches in a domain?

○ A) STP ● B) VTP

○ C) DHCP ○ D) ISL

1 points

13. When a router is connected to a Frame Relay WAN link using a serial DTE interface, how is the clock rate determined?

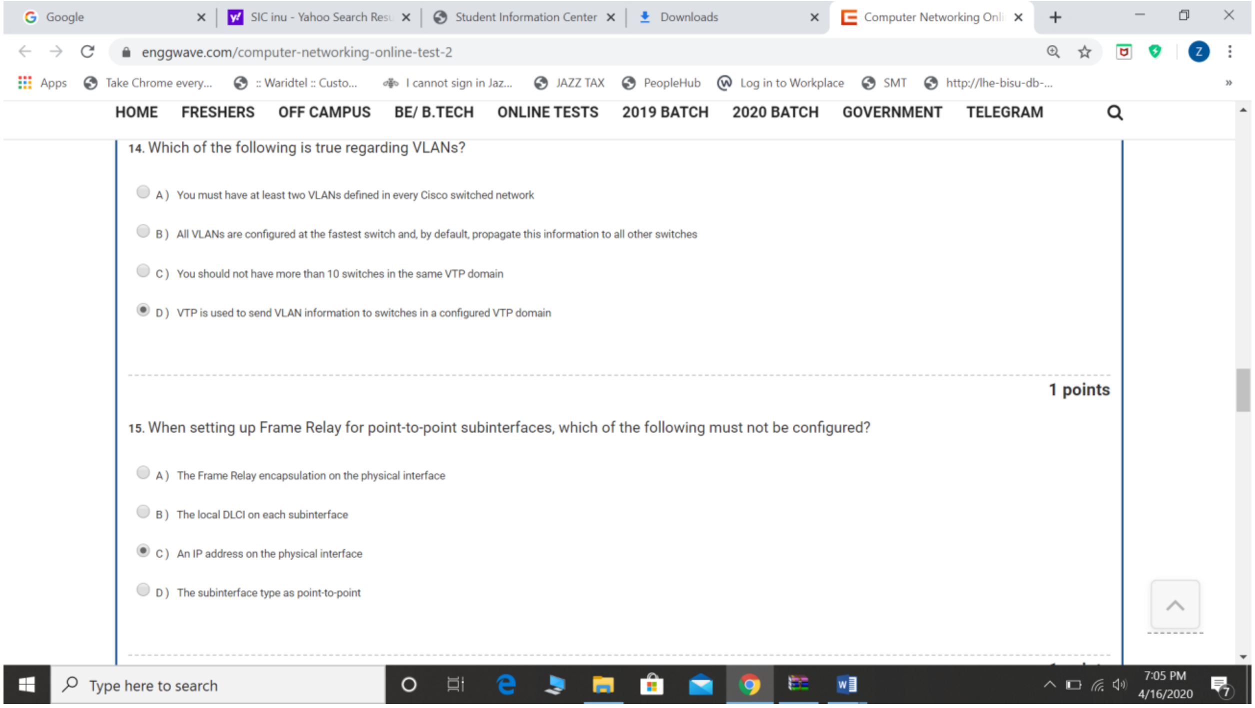
● A) Supplied by the CSU/DSU

○ B) By the far end router

○ C) By the clock rate command

○ D) By the Physical layer bit stream timing

1 points



14. Which of the following is true regarding VLANs?

○ A) You must have at least two VLANs defined in every Cisco switched network

○ B) All VLANs are configured at the fastest switch and, by default, propagate this information to all other switches

○ C) You should not have more than 10 switches in the same VTP domain

● D) VTP is used to send VLAN information to switches in a configured VTP domain

1 points

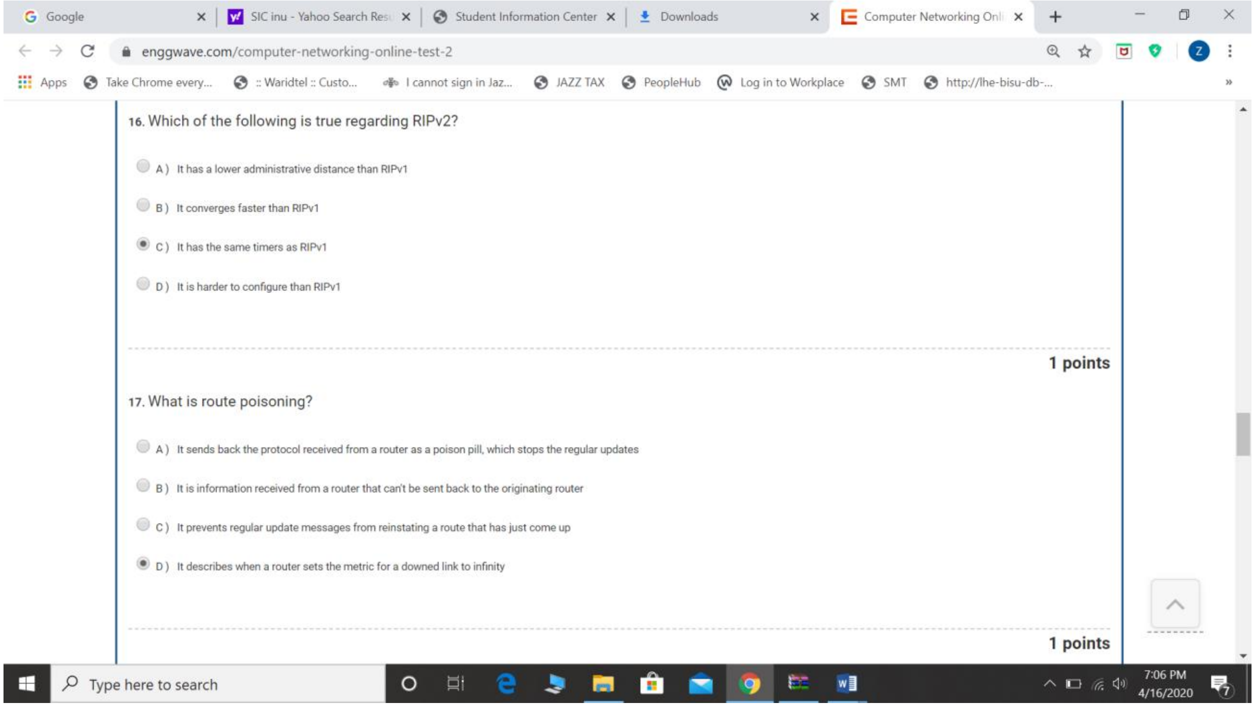
15. When setting up Frame Relay for point-to-point subinterfaces, which of the following must not be configured?

○ A) The Frame Relay encapsulation on the physical interface

○ B) The local DLCI on each subinterface

● C) An IP address on the physical interface

○ D) The subinterface type as point-to-point



16. Which of the following is true regarding RIPv2?

○ A) It has a lower administrative distance than RIPv1

○ B) It converges faster than RIPv1

● C) It has the same timers as RIPv1

○ D) It is harder to configure than RIPv1

1 points

17. What is route poisoning?

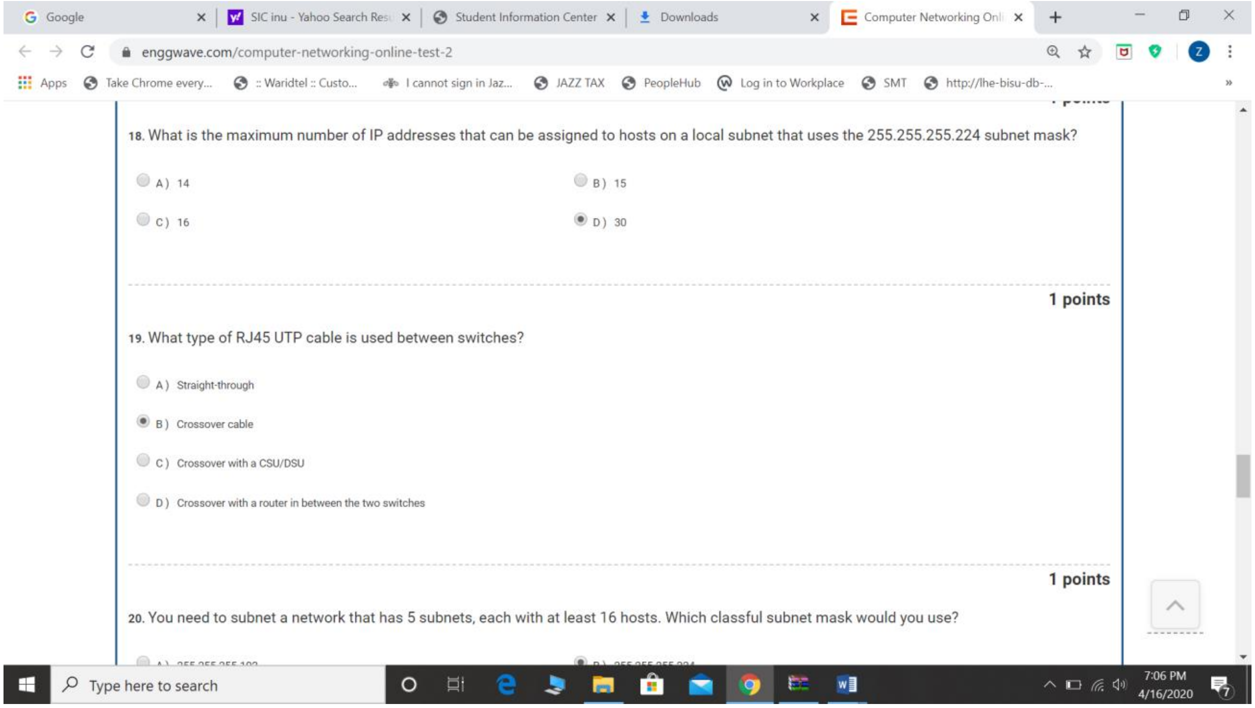
○ A) It sends back the protocol received from a router as a poison pill, which stops the regular updates

○ B) It is information received from a router that can't be sent back to the originating router

○ C) It prevents regular update messages from reinstating a route that has just come up

● D) It describes when a router sets the metric for a downed link to infinity

1 points



18. What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask?

○ A) 14 ○ B) 15

○ C) 16 ● D) 30

1 points

19. What type of RJ45 UTP cable is used between switches?

○ A) Straight-through

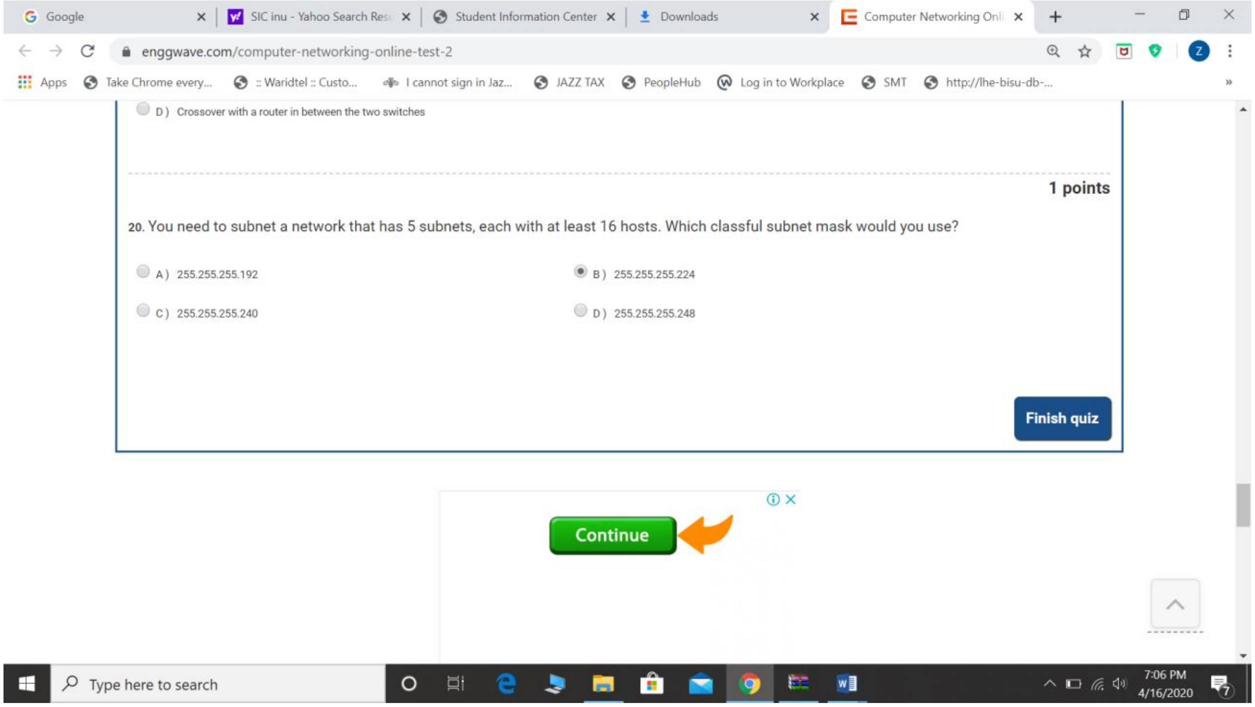
● B) Crossover cable

○ C) Crossover with a CSU/DSU

○ D) Crossover with a router in between the two switches

1 points

20. You need to subnet a network that has 5 subnets, each with at least 16 hosts. Which classful subnet mask would you use?



○ D) Crossover with a router in between the two switches

1 points

20. You need to subnet a network that has 5 subnets, each with at least 16 hosts. Which classful subnet mask would you use?

○ A) 255.255.255.192 ● B) 255.255.255.224

○ C) 255.255.255.240 ○ D) 255.255.255.248

Finish quiz