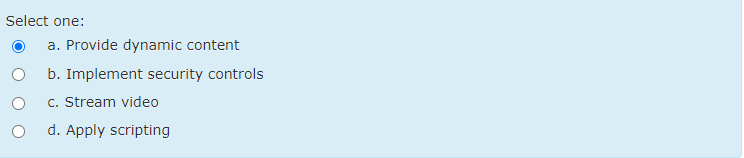
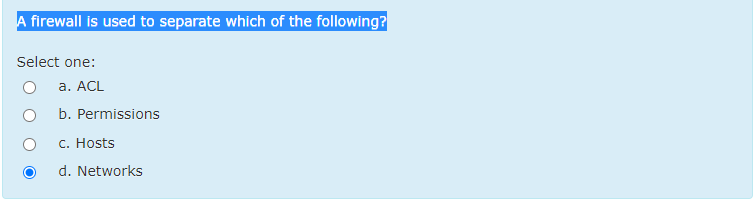
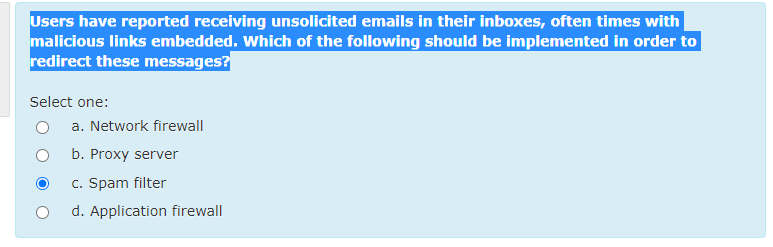
1. Web applications are used to



1. A firewall is used to separate which of the following?



1. **Users have reported receiving unsolicited emails in their inboxes, often times with malicious links embedded. Which of the following should be implemented in order to redirect these messages?**



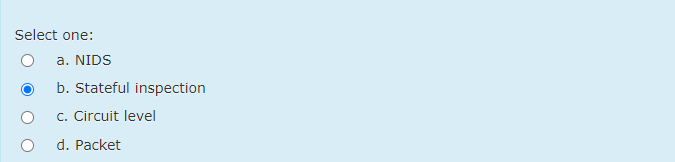
1. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number

Availability & Integrity

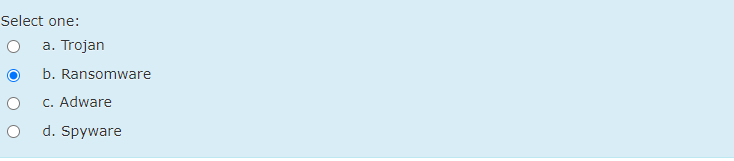
1. What is *not*a benefit of hardware keyloggers?

Difficult to install

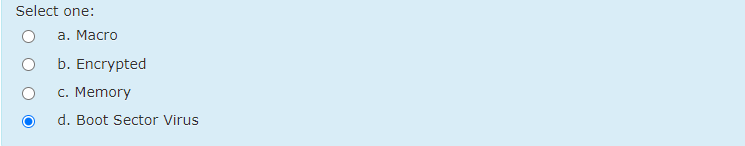
1. What type of firewall analyzes the status of traffic



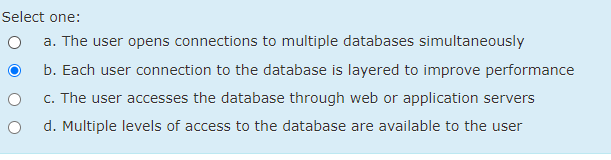
1. **A user, Ann, is reporting to the company IT support group that her workstation screen is blank other than a window with a message requesting payment or else her hard drive will be formatted. Which of the following types of malware is on Ann’s workstation?**



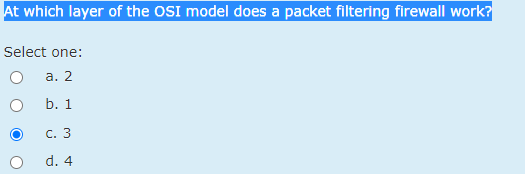
1. Which virus infects the master boot record and it is a complex task to remove this virus.



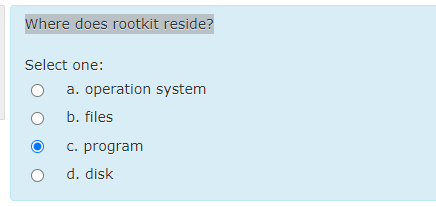
1. What does it mean for a user to access a database through a multi-tier infrastructure?



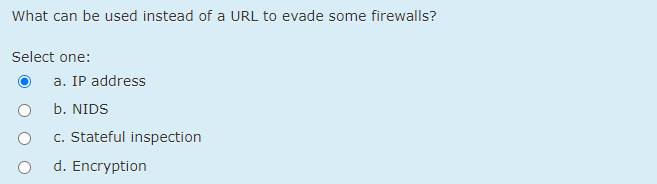
1. At which layer of the OSI model does a packet filtering firewall work?



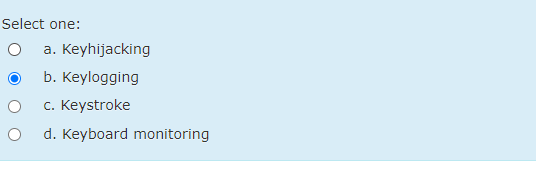
1. Where does rootkit reside?



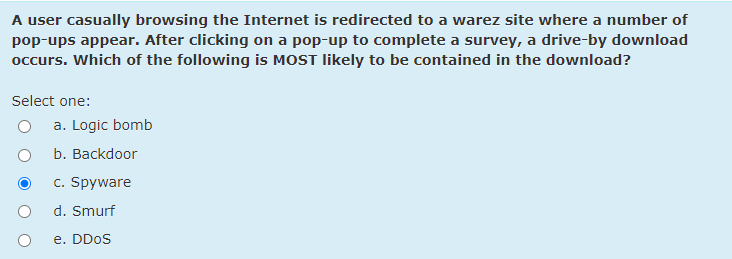
1. **What can be used instead of a URL to evade some firewalls?**



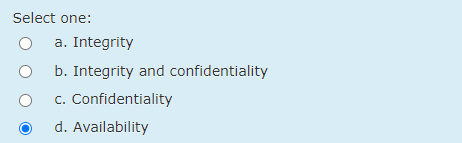
1. Which method of hacking will record all your keystrokes?

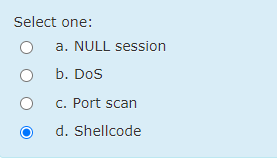


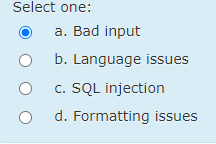
1. **A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?**



1. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name



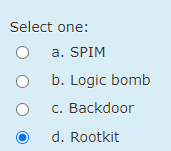
1. A …..is used to attack an Intrusion detection system
2. Input validation is used to prevent which of the following?



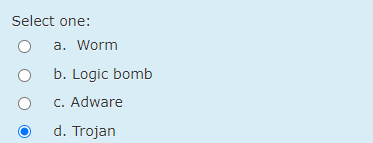
1. Which of the following is a scripting language?

CGI

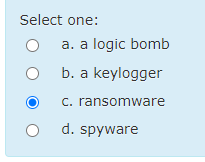
1. **During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running. Which of the following has MOST likely been installed on the server?**



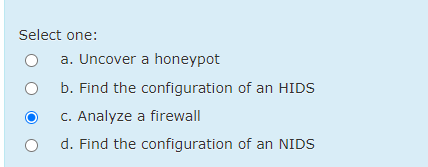
1. **Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?**



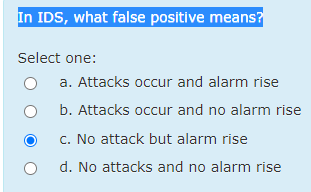
1. **After surfing the Internet, Joe, a user, woke up to find all his files were corrupted. His wallpaper was replaced by a message stating the files were encrypted and he needed to transfer money to a foreign country to recover them. Joe is a victim of:**



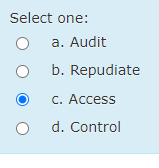
1. Firewalking is done to accomplish which of the following?

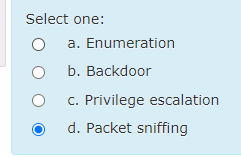


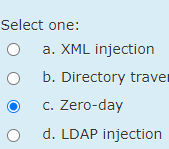
1. In IDS, what false positive means?



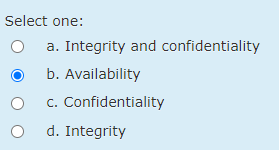
1. If a security mechanism offers availability, then it offers a high level of assurance that authorized subjects can \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ the data, objects, and resources.



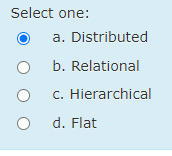
1. An NIDS is based on technology similar to which of the following
2. **Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?**



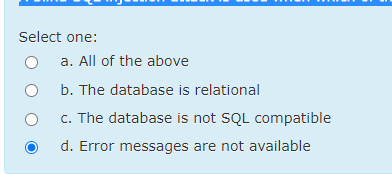
1. Paul crashes Linda's system. Which violation occur?



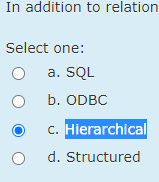
1. What type of database has its information spread across many disparate systems?



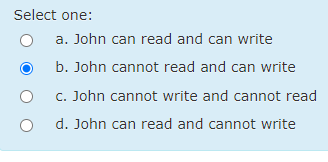
1. A blind SQL injection attack is used when which of the following is true?



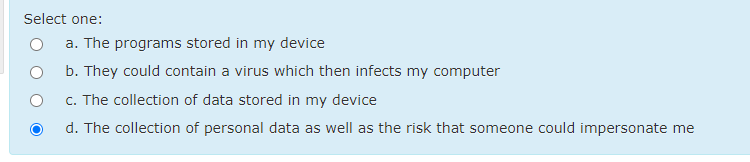
1. In addition to relational databases there is also what kind of database?



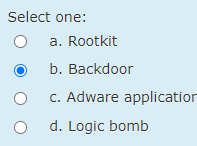
1. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (SECRET, {A, B}). John want to access to a document classified (TOP SECRET, {A, B, C})”. Which true statement?



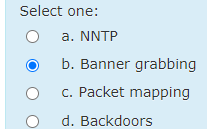
1. However cookies also raise some security and privacy concerns, for example…



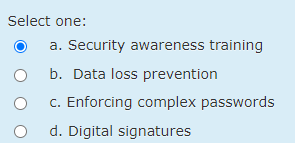
1. **A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:**



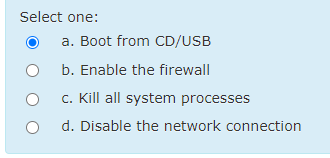
1. An attacker can use to find information about a firewall.



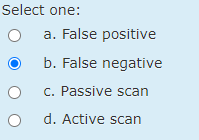
1. **Several employees clicked on a link in a malicious message that bypassed the spam filter and their PCs were infected with malware as a result. Which of the following BEST prevents this situation from occurring in the future?**



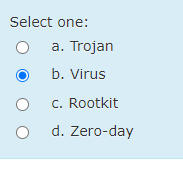
1. **A Windows- based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?**



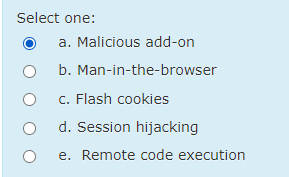
1. **Although a vulnerability scan report shows no vulnerabilities have been discovered, a subsequent penetration test reveals vulnerabilities on the network. Which of the following has been reported by the vulnerability scan?**



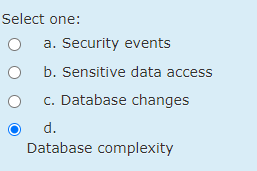
1. **A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone’s boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program?**



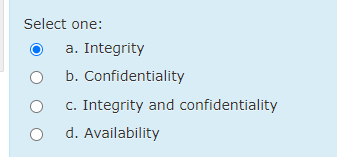
1. **A news and weather toolbar was accidently installed into a web browser. The toolbar tracks users online activities and sends them to a central logging server. Which of the following attacks took place?**



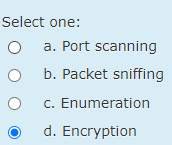
1. Which of the following does a database security solution **not**monitor?



1. Carol changes the amount of Angelo's check from $100 to $1,000. Which violation occur?



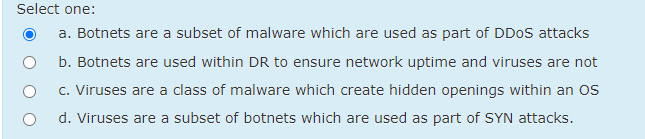
1. Which of the following can be used to evade an IDS?



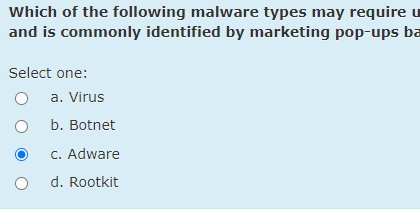
1. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (UNCLASSIFIED, {A, B}). John wants to access to a document classified (TOP SECRET, {A, B, C})”. Which true statement?

Can write cannot read0

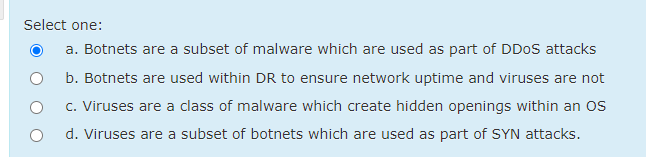
1. **Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?**



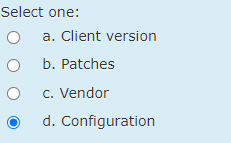
1. **Which of the following malware types may require user interaction, does not hide itself, and is commonly identified by marketing pop-ups based on browsing habits?**



1. **The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection. Which of the following has happened on the workstation?**



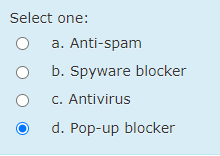
1. Databases can be a victim of code exploits depending on



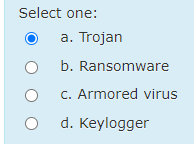
1. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (SECRET, {C}). John want to access to a document classified (TOP SECRET, {A, B})”. Which true statement?

Cannot read cannot write

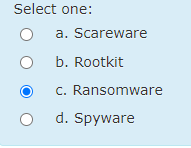
1. **A user has several random browser windows opening on their computer. Which of the following programs can be installed on his machine to help prevent this from happening?**



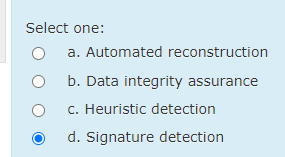
1. **Which of the following types of malware, attempts to circumvent malware detection by trying to hide its true location on the infected system?**



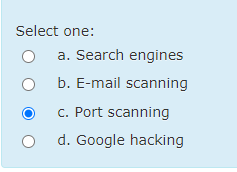
1. **An employee reports work was being completed on a company-owned laptop using a public wireless hot-spot. A pop-up screen appeared, and the user closed the pop-up. Seconds later, the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?**



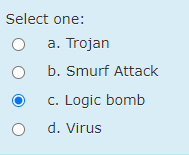
1. What is the most commonly used technique to protect against virus attacks?



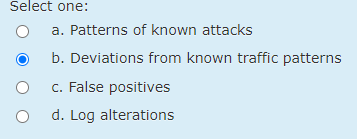
1. Which of the following can be used to identify a firewall?



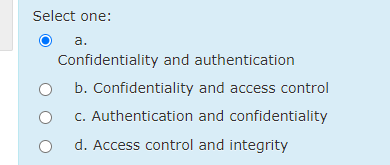
1. **The Chief Information Officer (CIO) receives an anonymous threatening message that says “beware of the 1st of the year”. The CIO suspects the message may be from a former disgruntled employee planning an attack. Which of the following should the CIO be concerned with?**



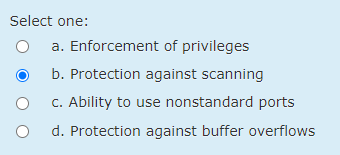
1. An anomaly-based NIDS is designed to look for what?



1. What policies they might be enforcing in this situation: "The permissions of the file containing Carol's homework will prevent Robert from cheating and copying it"



1. Which of the following challenges can be solved by firewalls?



1. Which of the following uses a database of known attacks

