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.pass4itsure.com/98-367.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following tools traces all or specific activities of a user on a computer?

A. Task Manager

B. Event Viewer

C. Network Monitor

D. Keylogger

Correct Answer: D

A keylogger is a software tool that traces all or specific activities of a user on a computer. Once a keylogger is installed on a victim\\'s computer, it can be used for recording all keystrokes on the victim\\'s computer in a predefined log file. An

attacker can configure a log file in such a manner that it can be sent automatically to a predefined e-mail address. Some of the main features of a keylogger are as follows:

It can record all keystrokes.

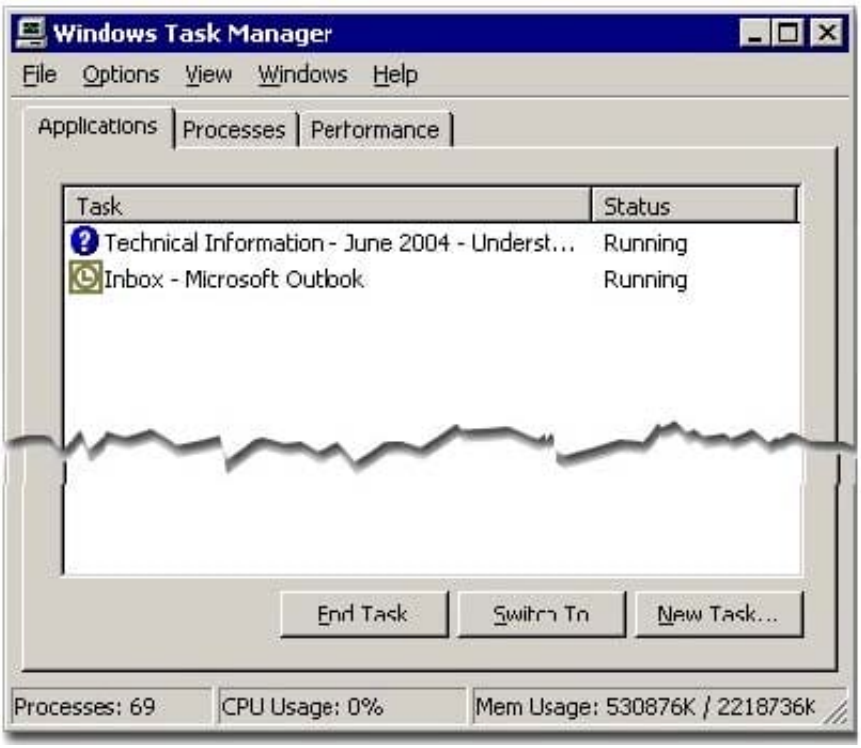
It can capture all screenshots.

It can record all instant messenger conversations. It can be remotely installed.

It can be delivered via FTP or e-mail.

Answer: A is incorrect. Task Manager is a utility that is used for managing applications, processes, and the general system performance and also for viewing the networking and user statistics. The Task Manager utility is used to run or end

programs or applications. Administrators use this tool to quickly identify and terminate a rogue application.



This utility can be run by invoking a Windows Security menu by using the Ctrl+Alt+Delkey combination and then clicking the Task Manager button or by right- clicking the task bar and then clicking the Task Managermenu option. Answer: B is

incorrect. Event Viewer is an administrative utility that displays the event log of a computer running Windows NT. Event Viewer displays the following categories of events:

Error: These events show significant problems, such as loss of data or loss of functionality. Warning: These events are not necessarily significant but indicate possible problems. Information: These events describe the successful operation of

an application, driver, or service. Success Audit: These events show successful audited security access attempts.

Failure Audit: These events show failed audited security access attempts. Answer: C is incorrect. Network Monitor (Netmon) is a protocol analyzer. It is used to analyze the network traffic. It is installed by default during the installation of the

operating system. It can be installed by using Windows Components Wizard in the Add or Remove Programs tool in Control Panel. Network Monitor is used to perform the following tasks:

1.Capture frames directly from the network.

2.Display and filter captured frames immediately after capture or a later time. 3.Edit captured frames and transmit them on the network.

4.Capture frames from a remote computer.

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

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 4

A brute force attack:

A. Uses response filtering

B. Tries all possible password variations

C. Uses the strongest possible algorithms

D. Targets all the ports

Correct Answer: B

QUESTION 5

The certificate of a secure public Web server on the Internet should be:

A. Issued by a public certificate authority (CA)

B. Signed by using a 4096-bit key

C. Signed by using a 1024-bit key

D. Issued by an enterprise certificate authority (CA)

Correct Answer: A