642-552

Cisco

Securing Cisco Networking Devices (SND)

642-552

QUESTION 1:

A malicious program is disguised as another useful program; consequently, when the user executes the program, files get erased and then the malicious program spreads itself using emails as the delivery mechanism. Which type of attack best describes how this scenario got started?

A. DoS
B. worm
C. virus
D. trojan horse
E. DDoS

Answer: D

Explanation:
Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.
A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include
* attempts to "flood" a network, thereby preventing legitimate network traffic
* attempts to disrupt connections between two machines, thereby preventing access to a service
* attempts to prevent a particular individual from accessing a service
* attempts to disrupt service to a specific system or person
Distributed Denial of Service
* An attacker launches the attack using several machines. In this case, an attacker breaks into several machines, or coordinates with several zombies to launch an attack against a target or network at the same time.
* This makes it difficult to detect because attacks originate from several IP addresses.
* If a single IP address is attacking a company, it can block that address at its firewall. If it is 300 00 this is extremely difficult.

QUESTION 2:

What is the key function of a comprehensive security policy?

A. informing staff of their obligatory requirements for protecting technology and information assets
B. detailing the way security needs will be met at corporate and department levels

C. recommending that Cisco IPS sensors be implemented at the network edge
D. detailing how to block malicious network attacks

Answer: A

Explanation:
Developing a strong security policy helps to protect your resources only if all staff members are properly instructed on all facets and processes of the policy. Most companies have a system in place whereby all employees need to sign a statement confirming that they have read and understood the security policy. The policy should cover all issues the employees encounter in their day-to-day work, such as laptop security, password policy, handling of sensitive information, access levels, tailgating, countermeasures, photo IDs, PIN codes, and security information delivered via newsletters and posters. A top-down approach is required if the policy is to be taken seriously. This means that the security policy should be issued and supported from an executive level downward.

QUESTION 3:

Which building blocks make up the Adaptive Threat Defense phase of Cisco SDN strategy?

A. VoIP services, NAC services, Cisco IBNS
B. network foundation protection, NIDS services, adaptive threat mitigation services
C. firewall services, intrusion prevention, secure connectivity
D. firewall services, IPS and network antivirus services, network intelligence
E. Anti-X defense, NAC services, network foundation protection

Answer: D

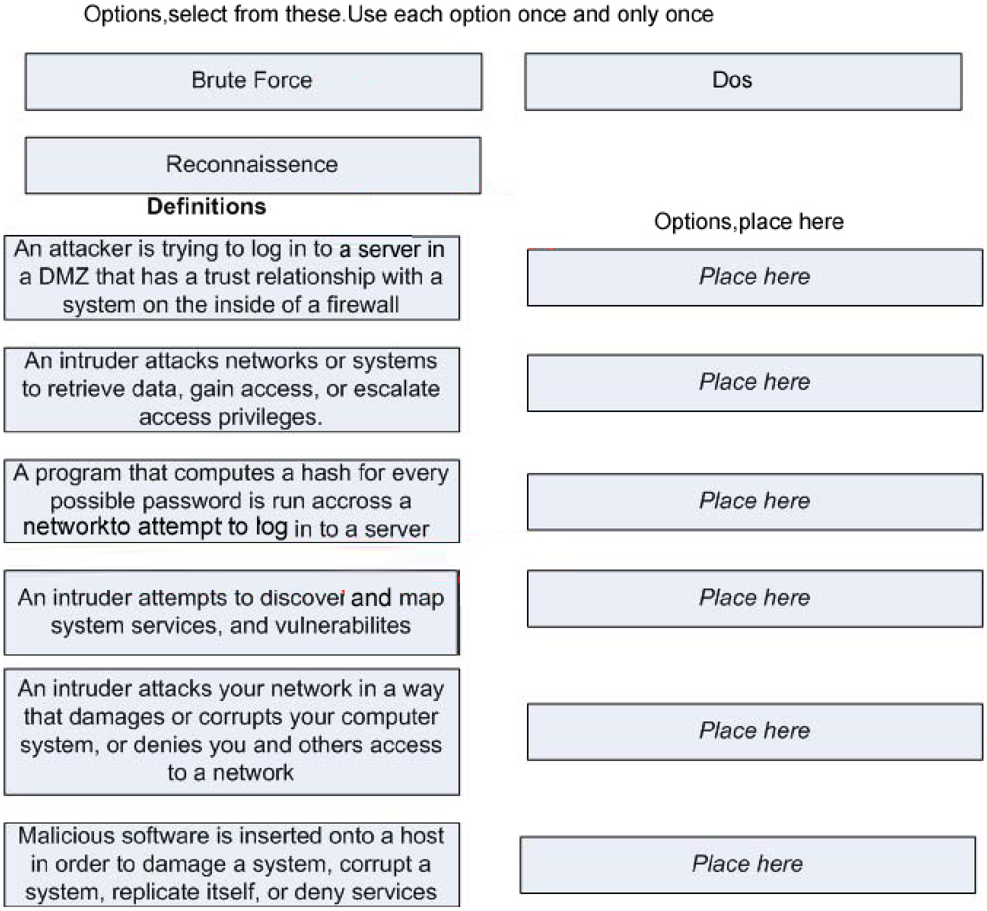
Explanation:
Computer connected to the Internet without a firewall can be hijacked and added to an Internet outlaw's botnet in just a few minutes. A firewall can block malware that could otherwise scan your computer for vulnerabilities and then try to break in at a weak point. The real issue is how to make one 99.9% secure when it is connected to in Internet. At a minimum computers need to have firewall, antivirus and anti-spyware software installed and kept up-to-date. A home network that uses a wired or wireless router with firewall features provides additional protection.
A computer virus can be best described as a small program or piece of code that penetrates into the operating system, causing unexpected and negative events to occur. A well-known example is a virus, SoBig. Computer viruses reside in the active memory of the host and try to duplicate themselves by different means. This duplication mechanism can vary from copying files and broadcasting data on local-area network (LAN) segments to sending copies via e-mail or an Internet relay chat (IRC). Antivirus software applications are developed to scan the memory and hard disks of hosts for known viruses.

If the application finds a virus (using a reference database with virus definitions), it informs the user.

QUESTION 4:

DRAG DROP

You work as a network administrator at Certkiller .com. Your boss Mrs. Certkiller asks you to match the malicious network attack types with the correct definition.



Options,select from these.Use each option once and only once

Brute Force

Dos

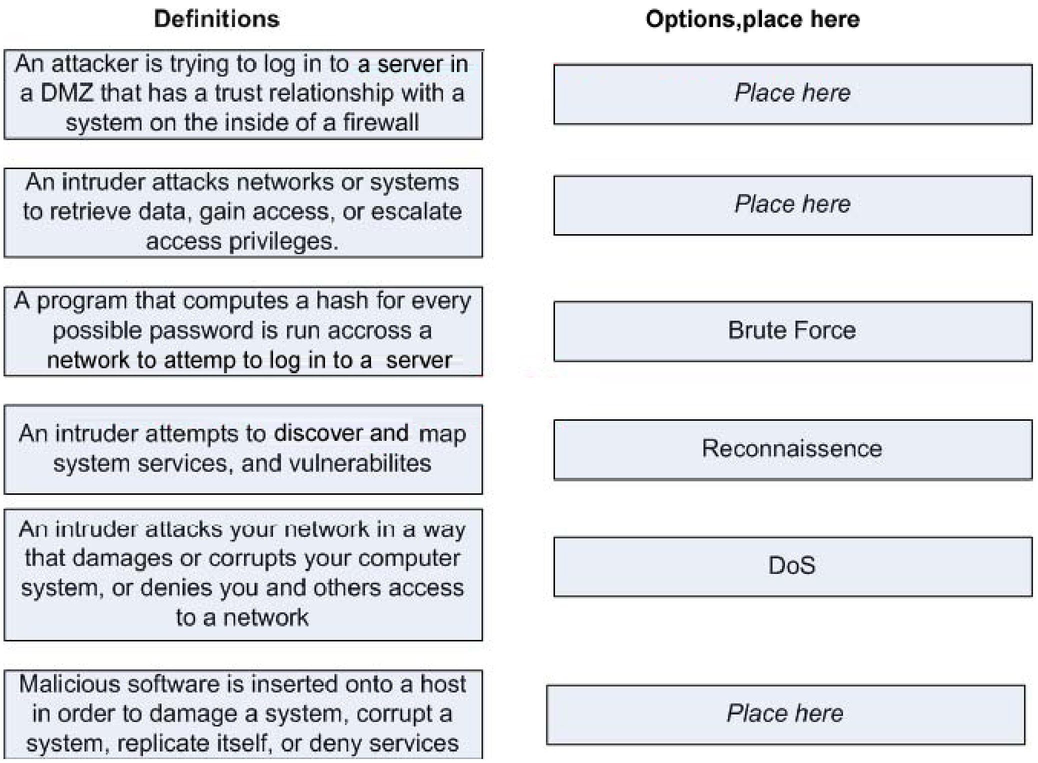
Reconnaissence

Definitions

Options,place here

Definitions	Options,place here
An attacker is trying to log in to a server in a DMZ that has a trust relationship with a system on the inside of a firewall	Place here
An intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.	Place here
A program that computes a hash for every possible password is run accross a networkto attempt to log in to a server	Place here
An intruder attempts to discover and map system services, and vulnerabilites	Place here
An intruder attacks your network in a way that damages or corrupts your computer system, or denies you and others access to a network	Place here
Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services	Place here

Answer:



Definitions	Options,place here
An attacker is trying to log in to a server in a DMZ that has a trust relationship with a system on the inside of a firewall	*Place here*
An intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.	*Place here*
A program that computes a hash for every possible password is run accross a network to attemp to log in to a server	Brute Force
An intruder attempts to discover and map system services, and vulnerabilites	Reconnaissence
An intruder attacks your network in a way that damages or corrupts your computer system, or denies you and others access to a network	DoS
Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services	*Place here*

Explanation:

1. Reconnaissance:

Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of attack prior to launching an attack. This phase is also where the attacker draws on competitive intelligence to learn more about the target. The phase may also involve network scanning either external or internal without authorization.

This is a phase that allows the potential attacker to strategize his attack. This may spread over time, as the attacker waits to unearth crucial information. One aspect that gains prominence here is social engineering. A social engineer is a person who usually smooths talk's people into revealing information such as unlisted phone numbers, passwords or even sensitive information. Other reconnaissance techniques include dumpster diving. Dumpster diving is the process of looking through an organization's trash for discarded sensitive information. Building user awareness of the precautions they must take in order to protect their information assets is a critical factor in this context.

2. DOS (Denial Of Service)

Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.

3. Brute force