Vendor: CompTIA

Exam Code:JK0-022

Exam Name: CompTIA Security+ Certification

Version: Demo

QUESTION 1

Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

A. HIPS

B. NIDS

C. HIDS

D. NIPS

Correct Answer: A

This question is asking which of the following is designed to stop an intrusion on a specific server. To stop an intrusion on a specific server, you would use a HIPS (Host Intrusion Prevention System). The difference between a HIPS and other intrusion prevention systems is that a HIPS is a software intrusion prevention systems that is installed on a `specific server\\'.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.

Incorrect Answers:

B: A NIDS (Network Intrusion Detection System) is typically a hardware device designed to detect intrusion attempts to the network, not a specific host. Therefore, this answer is incorrect.

C: A HIDS (Host Intrusion Detection System) is a host based system. However it is a `detection\\' system not a prevention system. Therefore it will only detect intrusion attempts; it will not stop them. Therefore, this answer is incorrect.

D: A NIPS (Network Intrusion Prevention System) is typically a hardware device designed to prevent intrusion attempts to the network, not a specific host. Therefore, this answer is incorrect.

References: http://en.wikipedia.org/wiki/Intrusion_prevention_system

---

QUESTION 2

After viewing wireless traffic, an attacker notices the following networks are being broadcasted by local access points:

Corpnet Coffeeshop FreePublicWifi

Using this information the attacker spoofs a response to make nearby laptops connect back to a malicious device. Which of the following has the attacker created?

A. Infrastructure as a Service

B. Load balancer

C. Evil twin

D. Virtualized network

Correct Answer: C

In this question, the attacker has created another wireless network that is impersonating one of more of the three wireless networks listed in the question. This is known as an Evil Twin. An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique. For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name. In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits.

Incorrect Answers:

A: Infrastructure as a Service is a term used to describe cloud based services hosted by cloud service providers. For example, a cloud provider might provide a web service. The cloud provider hosts the service on virtualized computers behind the scenes. As a customer, you just pay for web service without requiring knowledge of the hardware that the service is hosted on. This is not what is described in this question. Therefore, this answer is incorrect.

B: A load balancer distributes traffic between servers. For example, you could have two or more web servers hosting your corporate website. The DNS record for the website will point to the virtual IP of the load balancer. The load balancer will then share web requests between the web servers. This is not what is described in this question. Therefore, this answer is incorrect.

D: A virtualized network is a network created on physical servers running Hypervisor software such as Microsoft HyperV or VMware VSphere. Virtualized networks are also used by cloud service providers. A cloud service is a service running on virtual servers. This is not what is described in this question. Therefore, this answer is incorrect.

References: http://www.techopedia.com/definition/5057/evil-twin

---

QUESTION 3

Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

A. Rootkit

B. Logic bomb

C. Worm

D. Botnet

Correct Answer: B

This is an example of a logic bomb. The logic bomb is configured to `go off\\' or when Jane has left the company. A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic

bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool\\'s Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.

Incorrect Answers:

A: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker\\'s use; alter log files; attack other machines on the network; and alter existing system tools to escape detection. A rootkit is not what is described in this question. Therefore, this answer is incorrect.

C: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. A worm is not what is described in this question. Therefore, this answer is incorrect.

D: A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation. Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet\\'s operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules. A botnet is not what is described in the question. Therefore, this answer is incorrect. References: http://en.wikipedia.org/wiki/Logic_bomb http://searchmidmarketsecurity.techtarget.com/definition/rootkit http://en.wikipedia.org/wiki/Computer_worm http://en.wikipedia.org/wiki/Botnet

---

QUESTION 4

Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI model?

A. Packet Filter Firewall

B. Stateful Firewall

C. Proxy Firewall

D. Application Firewall

Correct Answer: B

Stateful inspections occur at all levels of the network.

Incorrect Answers:

A: Packet-filtering firewalls operate at the Network layer (Layer 3) and the Transport layer (Layer 4) of the Open Systems Interconnect (OSI) model.

C: The proxy function can occur at either the application level or the circuit level.

D: Application Firewalls operates at the Application layer (Layer7) of the OSI model.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 98-100.

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 6.

QUESTION 5

A security administrator wants to deploy security controls to mitigate the threat of company employees\\' personal information being captured online. Which of the following would BEST serve this purpose?

A. Anti-spyware

B. Antivirus

C. Host-based firewall

D. Web content filter

Correct Answer: A

Spyware monitors a user\\'s activity and uses network protocols to reports it to a third party without the user\\'s knowledge. This is usually accomplished using a tracking cookie.

Incorrect Answers:

B: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Computer viruses do not capture user information.

C: A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet.

D: Web content filtering is a form of content inspection in which the content of a web page is inspected against a blacklist of unwanted terms. This would not prevent user information being captured online.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 161-162, 300 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 19,

---

QUESTION 6

Which of the following defines a business goal for system restoration and acceptable data loss?

A. MTTR

B. MTBF

C. RPO

D. Warm site

Correct Answer: C

The recovery point objective (RPO) defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). This is an essential business goal insofar as system restoration and acceptable data loss is concerned.

Incorrect Answers:

A: The mean time to restore (MTTR) is the measurement of how long it takes to repair a system or component once a failure occurs. This means it has to do with TIME lost not data loss restoration per se.

B: The mean time between failures (MTBF) is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component\\'s anticipated lifetime. This is thus also a TIME issue.

D: A warm site provides some of the capabilities of a hot site; it must provide computer systems and compatible media capabilities.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9, 444

QUESTION 7

Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

A. Application patch management

B. Cross-site scripting prevention

C. Creating a security baseline

D. System hardening

Correct Answer: D

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

Incorrect Answers:

A: Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

B: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web

server, using firewalls, and auditing for suspicious activity.

C: A security baseline is the security setting of a system that is known to be secure. This is the initial security setting of a system. Once the baseline has been applied, it must be maintained or improved. Maintaining the security baseline requires continuous monitoring.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 61, 215-217, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 195, 207-208,

---

QUESTION 8

While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

A. Cross-site scripting

B. Buffer overflow

C. Header manipulation

D. Directory traversal

Correct Answer: B

When the user opens an attachment, the attachment is loaded into memory. The error is caused by a memory issue due to a buffer overflow attack.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user\\'s files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug- in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. As XSS is a web based attack, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

C: A header manipulation attack uses other methods (hijacking, cross-site forgery, and so forth) to change values in HTTP headers and falsify access. When used with XSRF, the attacker can even change a user\\'s cookie. Internet Explorer 8 and above include InPrivate Filtering to help prevent some of this. By default, your browser sends information to sites as they need it--think of requesting a map from a site; it needs to know your location in order to give directions. With InPrivate Filtering, you can configure the browser not to share information that can be captured and manipulated.

As header manipulation is a web based attack, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

D: Directory traversal is a form of HTTP exploit in which a hacker uses the software on a Web server to access data in a directory other than the server\\'s root directory. If the attempt is successful, the hacker can view restricted files or even execute commands on the server. Although some educated guesswork is involved in finding paths to restricted files on a Web server, a skilled hacker can easily carry out this type of attack on an inadequately protected server by searching through the directory tree. The risk of such attacks can be minimized by careful Web server programming, the installation of software updates and patches, filtering of input from browsers, and the use of vulnerability scanners. As directory traversal is a form of HTTP exploit, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

References:

http://searchsecurity.techtarget.com/definition/buffer-overflow http://en.wikipedia.org/wiki/Cross-site_scripting Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 340 http://

searchsecurity.techtarget.com/definition/directory-traversal

QUESTION 9

Which of the following secure file transfer methods uses port 22 by default?

A. FTPS

B. SFTP

C. SSL

D. S/MIME

Correct Answer: B

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Incorrect Answers:

A: FTPS uses ports 989 and 990.

C: SSL operates over TCP port 443.

D: S/MIME is an Internet standard for encrypting and digitally signing e-mail.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 45, 51, 313.

QUESTION 10

Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

A. Hardware load balancing

B. RAID

C. A cold site

D. A host standby

Correct Answer: B

Fault tolerance is the ability of a system to sustain operations in the event of a component failure. Fault-tolerant systems can continue operation even though a critical component, such as a disk drive, has failed. This capability involves overengineering systems by adding redundant components and subsystems. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

Incorrect Answers:

A: Balancing the load between multiple servers instead of relying on only one reduces the response time, maximizes throughput, and allows better allocation of resources. It does not mean withstanding hardware failure, it just means high

availability. It also adds costs and there is no budget.

C: A cold site is a facility that isn\\'t immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn\\'t usually the case; the site provides a place for

operations to resume, but it doesn\\'t provide the infrastructure to support those operations.

Thus no servers fault tolerance as is required.

D: A Host standby assumes that you need to purchase additional servers to act as a standby.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 33, 103, 444

QUESTION 11

The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

A. Warm site implementation for the datacenter

B. Geographically disparate site redundant datacenter

C. Localized clustering of the datacenter

D. Cold site implementation for the datacenter

Correct Answer: B

Data backups, redundant systems, and disaster recovery plans all support availability. AN in this case a geographically disparate site redundant datacenter represents 100% availability regardless of whether a disaster event occurs.

Incorrect Answers:

A: A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations.

C: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. In this case localized clustering does not guarantee 100 % availability in the event of a disaster occurring.

D: A cold site is a facility that isn\\'t immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn\\'t usually the case; the site provides a place for operations to resume, but it doesn\\'t provide the infrastructure to support those operations.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 414, 444

QUESTION 12

The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when typing to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure?

A. The access rules on the IDS

B. The pop up blocker in the employee\\'s browser

C. The sensitivity level of the spam filter

D. The default block page on the URL filter

Correct Answer: D

A URL filter is used to block access to a site based on all or part of a URL. There are a number of URL-filtering tools that can acquire updated master URL block lists from vendors, as well as allow administrators to add or remove URLs from a custom list.

Incorrect Answers:

A: An intrusion detection system (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations.

B: Pop-up blockers prevent websites from opening further web browser windows without your approval.

C: A spam filter deals with identifying and blocking/filtering/removing unsolicited messages.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 18, 19, 21, 246.