Free Questions for SSCP by go4braindumps

Shared by Hutchinson on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following technologies is a target of XSS or CSS (Cross-Site Scripting) attacks?

Options:

A- Web Applications

B- Intrusion Detection Systems

C- Firewalls

D- DNS Servers

Answer:

A

Explanation:

XSS or Cross-Site Scripting is a threat to web applications where malicious code is placed on a website that attacks the use using their existing authenticated session status.

Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

Mitigation:

Configure your IPS - Intrusion Prevention System to detect and suppress this traffic.

Input Validation on the web application to normalize inputted data.

Set web apps to bind session cookies to the IP Address of the legitimate user and only permit that IP Address to use that cookie.

See the XSS (Cross Site Scripting) Prevention Cheat Sheet

See the Abridged XSS Prevention Cheat Sheet

See the DOM based XSS Prevention Cheat Sheet

See the OWASP Development Guide article on Phishing.

See the OWASP Development Guide article on Data Validation.

The following answers are incorrect:

Intrusion Detection Systems: Sorry. IDS Systems aren't usually the target of XSS attacks but a properly-configured IDS/IPS can 'detect and report on malicious string and suppress the TCP connection in an attempt to mitigate the threat.

Firewalls: Sorry. Firewalls aren't usually the target of XSS attacks.

DNS Servers: Same as above, DNS Servers aren't usually targeted in XSS attacks but they play a key role in the domain name resolution in the XSS attack process.

The following reference(s) was used to create this question:

CCCure Holistic Security+ CBT and Curriculum

and

https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

Question 2

Question Type: **MultipleChoice**

What is malware that can spread itself over open network connections?

Options:

A- Worm

B- Rootkit

C- Adware

D- Logic Bomb

Answer:

A

Explanation:

Computer worms are also known as Network Mobile Code, or a virus-like bit of code that can replicate itself over a network, infecting adjacent computers.

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 notable example is the SQL Slammer computer worm that spread globally in ten minutes on January 25, 2003. I myself came to work that day as a software tester and found all my SQL servers infected and actively trying to infect other computers on the test network.

A patch had been released a year prior by Microsoft and if systems were not patched and exposed to a 376 byte UDP packet from an infected host then system would become compromised.

Ordinarily, infected computers are not to be trusted and must be rebuilt from scratch but the vulnerability could be mitigated by replacing a single vulnerable dll called sqlsort.dll.

Replacing that with the patched version completely disabled the worm which really illustrates to us the importance of actively patching our systems against such network mobile code.

The following answers are incorrect:

- Rootkit: Sorry, this isn't correct because a rootkit isn't ordinarily classified as network mobile code like a worm is. This isn't to say that a rootkit couldn't be included in a worm, just that a rootkit isn't usually classified like a worm. A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of 'root' (the traditional name of the privileged account on Unix operating systems) and the word 'kit' (which refers to the software components that implement the tool). The term 'rootkit' has negative connotations through its association with malware.

- Adware: Incorrect answer. Sorry but adware isn't usually classified as a worm. Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.

- Logic Bomb: Logic bombs like adware or rootkits could be spread by worms if they exploit the right service and gain root or admin access on a computer.

The following reference(s) was used to create this question:

The CCCure

CompTIA Holistic Security+ Tutorial and CBT

and

http://en.wikipedia.org/wiki/Rootkit

and

http://en.wikipedia.org/wiki/Computer_worm

and

http://en.wikipedia.org/wiki/Adware

Question 3

Question Type: **MultipleChoice**

Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:

Options:

A- Not possible

B- Only possible with key recovery scheme of all user keys

C- It is possible only if X509 Version 3 certificates are used

D- It is possible only by 'brute force' decryption

Answer:

A

Explanation:

Content security measures presumes that the content is available in cleartext on the central mail server.

Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central 'crypto mail server'.

There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

Question 4

Question Type: MultipleChoice

Layer 4 of the OSI stack is known as:

Options:

A- the data link layer

B- the transport layer

C- the network layer

D- the presentation layer

Answer:

B

Explanation:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

Question 5

Question Type: MultipleChoice

Why does fiber optic communication technology have significant security advantage over other transmission technology?

Options:

A- Higher data rates can be transmitted.

B- Interception of data traffic is more difficult.

C- Traffic analysis is prevented by multiplexing.

D- Single and double-bit errors are correctable.

Answer:

B

Explanation:

It would be correct to select the first answer if the world 'security' was not in the question.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

Question 6

Question Type: MultipleChoice

Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?

Options:

A- Inbound packets with Source Routing option set

B- Router information exchange protocols

C- Inbound packets with an internal address as the source IP address

D- Outbound packets with an external destination IP address

Answer:

D

Explanation:

Normal outbound traffic has an internal source IP address and an external destination IP address.

Traffic with an internal source IP address should only come from an internal interface. Such packets coming from an external interface should be dropped.

Packets with the source-routing option enabled usually indicates a network intrusion attempt.

Router information exchange protocols like RIP and OSPF should be dropped to avoid having internal routing equipment being reconfigured by external agents.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.

Question 7

Question Type: MultipleChoice

In the context of network enumeration by an outside attacker and possible Distributed Denial of Service (DDoS) attacks, which of the following firewall rules is not appropriate to protect an organization's internal network?

Options:

A- Allow echo reply outbound

B- Allow echo request outbound

C- Drop echo request inbound

D- Allow echo reply inbound

Answer:

A

Explanation:

Echo replies outbound should be dropped, not allowed. There is no reason for any internet users to send ICMP ECHO Request to your interal hosts from the internet. If they wish to find out if a service is available, they can use a browser to connect to your web server or simply send an email if they wish to test your mail service.

Echo replies outbound could be used as part of the SMURF amplification attack where someone will send ICMP echo requests to gateways broadcast addresses in order to amplify the request by X number of users sitting behind the gateway.

By allowing inbound echo requests and outbound echo replies, it makes it easier for attackers to learn about the internal network as well by performing a simply ping sweep. ICMP can also be used to find out which host has been up and running the longest which would indicates which patches are missing on the host if a critical patch required a reboot.

ICMP can also be use for DDoS attacks, so you should strictly limit what type of ICMP traffic would be allowed to flow through your firewall.

On top of all this, tools such as LOKI could be use as a client-server application to transfer files back and forward between the internat and some of your internal hosts. LOKI is a client/server program published in the online publication Phrack . This program is a working proof-of-concept to demonstrate that data can be transmitted somewhat secretly across a network by hiding it in traffic that normally does not contain payloads. The example code can tunnel the equivalent of a Unix RCMD/RSH session in either ICMP echo request (ping) packets or UDP traffic to the DNS port. This is used as a back door into a Unix system after root access has been compromised. Presence of LOKI on a system is evidence that the system has been compromised in the past.

The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.

The following answers are incorrect:

Allow echo request outbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.

Drop echo request inbound There is no need for anyone on the internet to attempt pinging your internal hosts.

Allow echo reply inbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.

Reference(s) used for this question:

http:// www.phrack.org/issues.html?issue=49&id=6

http:// www.phrack.org/issues.html?issue=49&id=6

STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.