QUESTION 899

Which process on a firewall makes permit/deny forwarding decisions based solely on address and service port information?

A. Circuit Proxy
B. Stateful Packet Inspection Proxy
C. Application Proxy
D. Transparency Proxy

Correct Answer: A

QUESTION 900

A proxy based firewall has which one of the following advantages over a firewall employing stateful packet inspection?

A. It has a greater throughput.
B. It detects intrusion faster.
C. It has greater network isolation.
D. It automatically configures the rule set.

Correct Answer: C

QUESTION 901

Firewalls filter incoming traffic according to

A. The packet composition.
B. A security policy.
C. Stateful packet rules.
D. A security process.

Correct Answer: B

QUESTION 902

Application Level Firewalls create:

A. a real circuit between the workstation client and the server
B. a virtual circuit between the workstation client and the server
C. an imaginary circuit between the workstation guest and the server
D. a temporary circuit between the workstation host and the server

Correct Answer: B

QUESTION 903

Which of the following is the biggest concern with firewall security?

A. Internal hackers.
B. Complex configuration rules leading to misconfiguration.
C. Buffer overflows.
D. Distributed denial of service (DDOS) attacks.

Correct Answer: B

QUESTION 904

Which of the following is true of network security?

A. A firewall is not a necessity in today's connected world.
B. A firewall is a necessity in today's connected world.
C. A whitewall is a necessity in today's connected world.
D. A black firewall is a necessity in today's connected world.

Correct Answer: B

QUESTION 905

Which of the following statements pertaining to firewalls is incorrect?

A. Firewall create bottlenecks between the internal and external network.
B. Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
C. Strong firewalls can protect a network at all layers of the OSI models.
D. Firewalls are used to create security checkpoints at the boundaries of private networks.

Correct Answer: C

QUESTION 906

Which of the following is the least important security service provided by a firewall?

A. Packet filtering
B. Encrypted tunnels
C. Network Address Translation
D. Proxy services

Correct Answer: B

QUESTION 907

Which of the following firewall rules is less likely to be found on a firewall installed between an organization's internal network and internet?

A. Permit all traffic to and from local host.
B. Permit all inbound ssh traffic.
C. Permit all inbound tcp connections.
D. Permit all syslog traffic to log-server.abc.org.

Correct Answer: C

QUESTION 908

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

A. Inbound packets with Source Routing option set.
B. Router information exchange protocols.
C. Inbound packets with an internal source IP address.
D. Outbound packets with an external destination IP address.

Correct Answer: D

QUESTION 909

By examining the "state" and "context" of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC). This type of firewall system is used in:

A. first generation firewall systems
B. second generation firewall systems
C. third generation firewall systems
D. fourth generation firewall systems

Correct Answer: C

QUESTION 910

Which of the following statements pertaining to packet filtering is incorrect?

A. It is based on ACLs.
B. It is not application dependant.
C. It operates at the network layer.
D. It keeps track of the state of a connection.

Correct Answer: D

QUESTION 911

A screening router can perform packet filtering based upon what data?

A. Translated source destination addresses.
B. Inverse address resolution.
C. Source and destination port number.
D. Source and destination addresses and application data.

Correct Answer: C

QUESTION 912

Why are hardware security features preferred over software security features?

A. They lock in a particular implementation.
B. They have a lower meantime to failure.
C. Firmware has fever software bugs.
D. They permit higher performance.

Correct Answer: D

QUESTION 913

Firewalls can be used to

A. Enforce security policy.
B. Protect data confidentiality.
C. Protect against protocol redirects.
D. Enforce Secure Network Interface addressing.

Correct Answer: A

QUESTION 914

Which one of the following operations of a secure communication session cannot be protected?

A. Session initialization
B. Session support
C. Session termination
D. Session control

Correct Answer: B

QUESTION 915

The general philosophy for DMZ's are that:

A. any system on the DMZ can be compromised because it's accessible from the Internet
B. any system on the DMZ cannot be compromised because it's not accessible from the Internet
C. some systems on the DMZ can be compromised because they are accessible from the Internet
D. any system on the DMZ cannot be compromised because it's by definition 100% safe and not accessible from the Internet

Correct Answer: A

QUESTION 916

What is NOT an authentication method within IKE and IPsec:

A. CHAP
B. Pre-shared Key
C. certificate based authentication
D. Public Key authentication

Correct Answer: A

QUESTION 917

In IPSec, if the communication mode is gateway-gateway or host-gateway:

A. Only tunnel mode can be used.
B. Only transport mode can be used.
C. Encapsulating Security Payload (ESP) authentication must be used.
D. Both tunnel and transport mode can be used.

Correct Answer: D

QUESTION 918

Internet Protocol Security (IPSec) provides security service within the Internet Protocol (IP) by doing all of the following EXCEPT

A. Enabling a system to select required security protocols.
B. Providing traffic analysis protection.