Question 23

Not yet answered

Marked out of 1

Flag question

NAT is a routing technology but when combined with a firewall it is considered a firewall technology instead.

Select one:

- True
- False

Question 24

Not yet answered

Marked out of 1

Flag question

Application proxy configured as a web proxy prohibit FTP, telnet or other traffic.

Select one:

- True
- False

Question 13

Not yet answered

Marked out of 2

Flag question

The best practice only is use a layered defense by deploying one IDS in front of the firewall

Select one:

- True
- False

Question 14

Not yet answered

Marked out of 1

Flag question

In.....it can acts as a firewall filtering technique where it allows only connections which originate on the inside network and will block the connections which originate on the outside network.

- a. Virtual Private Network Firewall.
- b. Network Address Translation Firewall.
- c. Application Level Firewall.
- d. Application Proxy Firewall.

.....is an intrusion detection mechanism that is designed by each organizations security policy.its settings can change to make appropriate changes to its functionality.

- a. Network Based Intrusion Detection System.
- b. System Intrusion Detection System.
- c. Firewall.
- d. Signature Recognition.

Software Firewall is used to filter traffic for individual home users.

Select one:

- True
- False

.....identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

- a. IDS
- b. IDS and IPS
- c. IPS
- d. None of the answers are true

7

d

ut of

Presence of rogue suid and sgid files on your Linux system that dose not match your master list of suid and sgid files could indicate an attack is related to.....

- a. System Intrusions.
- b. File System Intrusions.
- c. File System Intrusions and Network Intrusions.
- d. Network Intrusions.

Question 1

Not yet answered

Marked out of 2

Flag question

..... is considered to reduce the security risks and increased the level of security controls.

- a. Hardware and Software firewall security .
- b. None of the answers are true.
- c. Hardware firewall security.
- d. Software firewall security.

Clear my choice

Question 2

Answer saved

Marked out of 2

Flag question

No Attack-Alert is refer to.....

- a. True Negative.
- b. True positive.
- c. False positive.
- d. False Negative.

Clear my choice

Question 3

Answer saved

Marked out of 2

Flag question

It detects the intrusion based on fixed behavioral characteristics of the users.....

- a. Protocol Anomaly Detection and Anomaly Detection
- b. Anomaly Detection
- c. Protocol Anomaly Detection
- d. Signature Recognition

Clear my choice

Question 4

Answer saved

Marked out of 2

Flag question

The presence of new unfamiliar programs indication intrusion related to.....

- a. File System Intrusions.
- b. All the answers are true.
- c. System Intrusions.
- d. Network Intrusions.

Clear my choice

Question 5

Answer saved

Marked out of 2

Flag question

.....can detect known attacks and there is a possibility that other innocuous packets might also contain the same signature, which will trigger a false positive alert.

- (●) a. Signature Recognition.
- ( ) b. All the answers are true.
- ( ) c. Protocol Anomaly Detection.
- ( ) d. Anomaly Detection.

Clear my choice

Question 6

Answer saved

Marked out of 2

Flag question

.....it helps to protect system from outside attempts of unauthorized access and protect against everyday email worms and Trojans.

- ( ) a. Software Firewall
- ( ) b. Screened Subnet Firewall.
- (●) c. All the answers are true.
- ( ) d. Hardware Firewall

Clear my choice

Question 7

Answer saved

Marked out of 2

Flag question

.....contains hosts that offer public services and has no hosts accessed by the private network.

- a. Multi homed Firewall.
- b. None of the answers are true.
- c. Screened Subnet.
- d. Bastion Host.

Clear my choice

Question 8

Answer saved

Marked out of 2

Flag question

Tripwire is an example of a log file monitoring tool.

Select one:

- True
- False

Question 9

Answer saved

Marked out of 2

Flag question

An intrusion detection system dose not raise an alarm when a legitimate attack has taken place is refer to.....

- a. True Negative.
- b. True positive.
- c. False positive.
- d. False Negative.

Clear my choice

Question 10

Answer saved

Marked out of 1

Flag question

Before deploying the IDS, it is essential to.....

- a. All the answers are true.
- b. Identify the critical components and Understand how the traffic flows.
- c. Analyze network topology.
- d. Identify the critical components and Analyze network topology.

Clear my choice

Question 11

Answer saved

Marked out of 2

Flag question

The .....typically consist of a black box that is placed in a promiscuous mode, listening for patterns indicative of an intrusion.

- a. Network Based Intrusion Detection Systems.
- b. File Based Intrusion Detection Systems.
- c. Host Based Intrusion Detection Systems.
- d. File System Intrusion Based Intrusion Detection Systems.

Clear my choice

Question 12

Answer saved

Marked out of 2

Flag question

Host Based Intrusion Detection System can configure to check inbound traffic at a "checkpoint",where a security audit is performed.

Select one:

- True
- False

Question 13

Answer saved

Marked out of 2

Flag question

In IDPSs Information is usually recorded globally, and might also be sent to separate systems such as centralized logging servers.

Select one:

- (●) True
- ( ) False

Question 14

Not yet answered

Marked out of 1

Flag question

Which of the following is not considered the disadvantage of the application proxy firewall?

- ( ) a. The services my use different servers.
- ( ) b. The services may require changes in the client and applications.
- (●) c. The services hides all the traffic that flows over it and ensures encryption.
- ( ) d. The services lag behind non proxy services until the suitable proxy software is available.

Clear my choice

Question 15

Answer saved

Marked out of 1

Flag question

.....work at the network layer of the OSI model and they are usually a part of a router.

- a. Application Level Firewall.
- b. Stateful Multilayer Inspection Firewall.
- c. Packet Filtering Firewall.
- d. Circuit-level Gateway Firewall.

Clear my choice

Question 16

Answer saved

Marked out of 1

Flag question

.....work at the session layer of the OSI model and they monitor requests to create sessions and determine if those session will be allowed.

- a. Virtual Private Network.
- b. Circuit level Gateway Firewall.
- c. Packet Filtering Firewall.
- d. Stateful Multilayer Inspection Firewall

Clear my choice

Question 17

Answer saved

Marked out of 1

Flag question

.....used to check whether or not the packet is coming from an unreliable zone.

- a. Interface.
- b. Destination TCP/UDP port.
- c. Direction.
- d. TCP flag bits.

Clear my choice

Question 18

Answer saved

Marked out of 1

Flag question

.....Used to check whether the protocol that the packet is carrying should be allowed.

- a. Source IP address.
- b. Interface.
- c. Direction.
- d. Protocol in use.

Clear my choice

Question 19

Answer saved

Marked out of 1

Remove flag

Each firewall service provides security depending on its efficiency and.....

- a. application.
- b. gateways.
- c. sophistication.
- d. translation.

Clear my choice

Question 20

Answer saved

Marked out of 1

Flag question

.....they filter packets at the network layer of the OSI model to determine whether session packets are legitimate and they evaluate the contents of packets at the application layer.

- a. Application Level Firewall.
- b. Stateful Multilayer Inspection Firewall.
- c. Network Address Translation firewall.
- d. Circuit level Gateway Firewall.

Clear my choice

Question 21

Answer saved

Marked out of 1

Flag question

In the.....incoming and outgoing traffic is restricted to services supported by proxy and all other service requests are denied.

- a. Application Level Firewall.
- b. Application Proxy.
- c. Circuit level Gateway Firewall.
- d. Stateful Multilayer Inspection Firewall.

Clear my choice

Question 22

Answer saved

Marked out of 1

Flag question

Anomaly detection is also known as misuse detection.

Select one:

- True
- False

Question 23

Not yet answered

Marked out of 1

Flag question

A firewall is unable to understand tunneled traffic.

Select one:

- True
- False

Question 24

Answer saved

Marked out of 1

Flag question

Application proxy configured as a web proxy prohibit FTP, telnet or other traffic.

Select one:

- True
- False