Prof. Amit Kumar Manjhvar

Quiz navigation

1 2 3 4 5 6 7 8
9 10

Show one page at a time
Finish review

Started on	Friday, 16 August 2024, 6:21 PM
State	Finished
Completed on	Friday, 16 August 2024, 6:31 PM
Time taken	9 mins 56 secs

Question **1**
Complete
Marked out of 1.00
Flag question

What are the major components of the intrusion detection system?

● a. All of the mentioned

○ b. Alert Database

○ c. Event provider

○ d. Analysis Engine

Your answer is correct.

Question **2**
Complete
Marked out of 1.00
Flag question

A packet Passes through a host running IP Tables. (The host is neither a source nor a sink for that packet) such a packet encounters the following chains in that host

(I). INPUT

(II). OUTPUT

(III). PREROUTING

(IV). POST ROUTING

(V). FORWARD

○ a. II & III

○ b. I & II

● c. III, IV & V

○ d. II , III & IV

Your answer is correct.

Question **3**
Complete
Marked out of 1.00
Flag question

What are the characteristics of anomaly based IDS?

○ a. It doesn't detect novel attacks

○ b. It detects based on signature

○ c. Anything distinct from the noise is not assumed to be intrusion activity

● d. It models the normal usage of network as a noise characterization

Your answer is correct.

Question **4**
Complete
Marked out of 1.00
Flag question

What are the different ways to classify an IDS?

○ a. signature based misuse

○ b. anomaly detection

● c. all of the mentioned

○ d. stack based

Your answer is correct.

Question **5**
Complete
Marked out of 1.00
Flag question

Which of the following operations is/are performed in the INPUT chain of IP tables?

(i). NAT

(ii). Filter

(iii). Route

(iv). Mangle

○ a. (ii) & (iii)

○ b. only(i)

○ c. only(ii)

● d. (ii) & (iv)

Your answer is correct.

Question **6**
Complete
Marked out of 1.00

Which of the following may be performed by the linux firewall, IP Tables?

○ a. filtering on MAC address

○ b. traffic rate limiting

Flag question

○ b. traffic rate limiting

○ c. Authentication

● d. Stateful packet Inspection

Your answer is correct.

Question **7**
Complete
Marked out of 1.00
Flag question

Information security system must be protected. In case of an attack, it must:

○ a. None of the above

○ b. do nothing

○ c. Shutdown once the attack is confirmed

● d. Provide enough information to assess the damage caused by the attack.

Your answer is correct.

Question **8**
Complete
Marked out of 1.00
Flag question

What are the different ways to classify an IDS?

○ a. Network & Zone based

○ b. Level based

● c. Host & Network based

○ d. Zone based

Your answer is correct.

Question **9**
Complete
Marked out of 1.00
Flag question

which of the following is/are usually placed in the outer DMZ of an organization?

● a. Web server

○ b. Application Server

○ c. Database Server

○ d. Authentication Server

Your answer is correct.

Question **10**
Complete
Marked out of 1.00
Flag question

What is the major drawback of anomaly detection IDS?

○ a. These are very slow at detection

○ b. It doesn't detect novel attacks

● c. It generates many false alarms

○ d. None of the mentioned

Your answer is correct.

Finish review

◄ QUIZ 1

Jump to...