[Updated Constantly]

HERE

CCNA Security v2.0 Chapter 5 Exam Answers

How to find: Press “Ctrl + F” in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **In configuring a Cisco router to prepare for IPS and VPN features, a network administrator opens the file realm-cisco.pub.key.txt, and copies and pastes the contents to the router at the global configuration prompt. What is the result after this configuration step?**
   - The router is authenticated with the Cisco secure IPS resource web server.
   - A pair of public/secret keys is created for IPsec VPN operation.
   - **A crypto key is created for IOS IPS to verify the master signature file.***
   - A pair of public/secret keys is created for the router to serve as an SSH server.

   The third step in implementing IOS IPS is to configure the Cisco IOS IPS public key that is located in the realm-cisco.pub.key.txt file. This public key is used to verify digital signature for the master signature file, and can be downloaded from cisco.com. To configure the IOS IPS crypto key, open the text file, and copy and paste the contents to the router at the global configuration prompt. Public/private key pairs for IPsec VPN and SSH server are generated using different methods.

2. **Which two benefits does the IPS version 5.x signature format provide over the version 4.x signature format? (Choose two.)**
   - support for IPX and AppleTalk protocols
   - addition of signature micro engines
   - support for comma-delimited data import
   - **support for encrypted signature parameters***
   - **addition of a signature risk rating***

   Since IOS 12.4(11)T, Cisco introduced version 5.x IPS signature format. The new version supports encrypted signature parameters and other features such as signature risk rating, which rates the signature on security risk.

3. **What information must an IPS track in order to detect attacks matching a composite signature?**
   - the total number of packets in the attack
   - the attacking period used by the attacker
   - the network bandwidth consumed by all packets
   - **the state of packets related to the attack***

   A composite signature is called a stateful signature. It identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time. Because this type of attack involves multiple packets, an IPS sensor must maintain the state information. However, an IPS sensor cannot maintain the state information indefinitely. A composite signature is configured with a time period to maintain the state for the specific attack when it is first detected. Thus, an IPS may not be able to maintain all the information related to an attack such as total number of packets, total length of attack time, and the amount of bandwidth consumed by the attack.

4. **What is a disadvantage of a pattern-based detection mechanism?**
   - The normal network traffic pattern must be profiled first.
   - **It cannot detect unknown attacks.***
   - It is difficult to deploy in a large network.
   - Its configuration is complex.

   An IDS/IPS with pattern-based detection, also known as signature-based detection, compares the network traffic to a database of known attacks (signature files) and triggers an alarm or prevents communication if a match is found. The signatures must be created first. Hence this type of intrusion detection cannot detect unknown attacks. It is easy to configure and to deploy. Its operation does not depend on the information of normal network behavior (or baseline).

5. **Which type of IPS signature detection is used to distract and confuse attackers?**
   - **honeypot-based detection***
   - policy-based detection
   - pattern-based detection
   - anomaly-based detection

   The honeypot-based detection method uses dummy servers to attract attacks. The purpose of the honey pot approach is to distract attacks away from real network devices. After capturing the attack activities on honeypot servers, network administrators can analyze incoming types of attacks and malicious traffic patterns.

6. **What is the purpose in configuring an IOS IPS crypto key when enabling IOS IPS on a Cisco router?**
   - to secure the IOS image in flash
   - to enable Cisco Configuration Professional to be launched securely
   - to encrypt the master signature file
   - **to verify the digital signature for the master signature file***

   The crypto key verifies the digital signature for the master signature file (sigdef-default.xml). The content of the file is signed by a Cisco private key to guarantee its authenticity and integrity.

7. **Refer to the exhibit. What is the result of issuing the Cisco IOS IPS commands on router R1?**

```
R1(config)# ip ips name iosips list 101
R1(config)# interface S0/0/0
R1(config-if)# ip ips iosips in
```

   - **All traffic that is permitted by the ACL is subject to inspection by the IPS.***
   - A named ACL determines the traffic to be inspected.
   - All traffic that is denied by the ACL is subject to inspection by the IPS.
   - A numbered ACL is applied to S0/0/0 in the outbound directio

   In configuring IOS IPS with the command ip ips, an optional extended or standard ACL can be used to filter the scanned traffic. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

8. **A system analyst is configuring and tuning a recently deployed IPS appliance. By examining the IPS alarm log, the analyst notices that the IPS does not generate alarms for a few known attack packets. Which term describes the lack of alarms by the IPS?**
   - true negative
   - false positive
   - **false negative***
   - true positive

   The alarms generated by an IPS can be classified into 4 types:
   A false positive occurs when an IPS generates an alarm on normal user traffic that should not have triggered an alarm.
   A false negative occurs when an IPS fails to generate an alarm after processing attack traffic the IPS is configured to detect.

A true positive occurs when an IPS generates an alarm in response to known attack traffic.
A true negative occurs when normal network traffic does not generate an alarm.

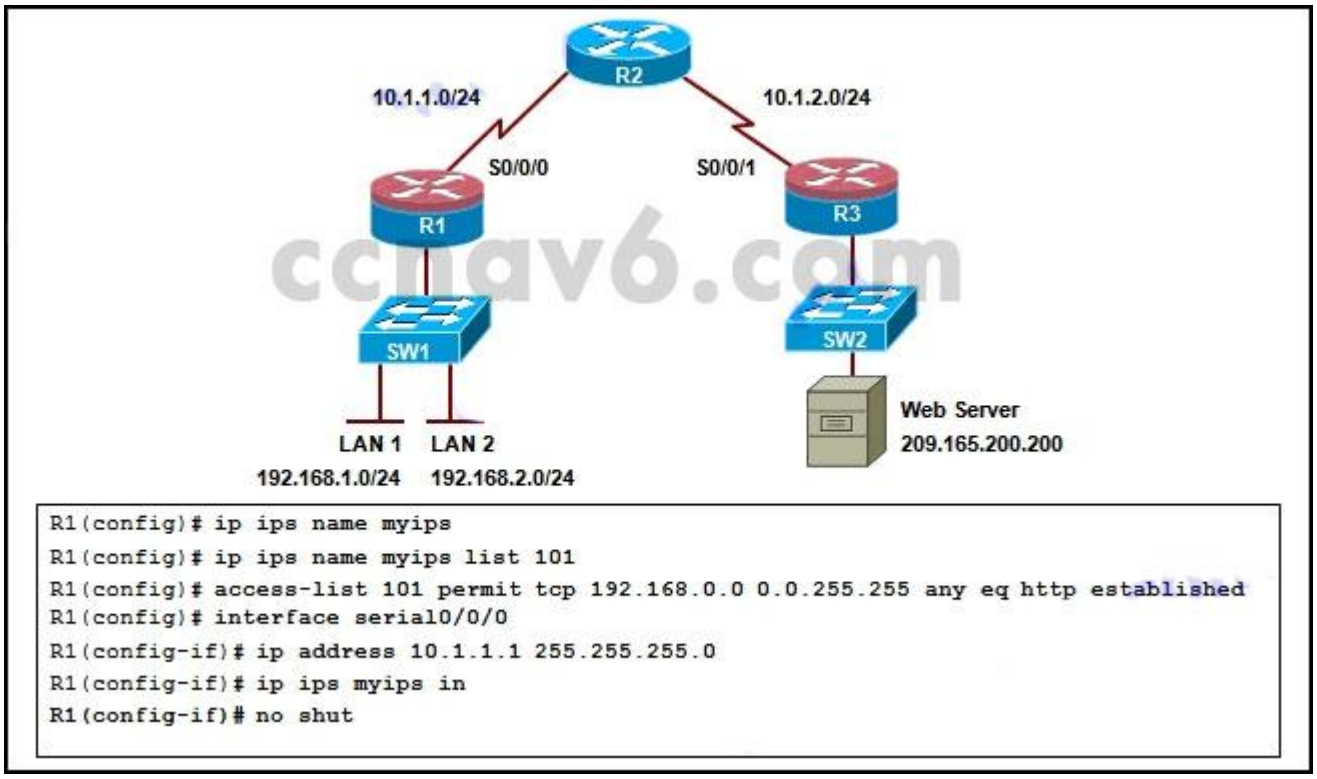
9. **A security specialist configures an IPS so that it will generate an alert when an attack is first detected. Alerts for the subsequent detection of the same attack are suppressed for a pre-defined period of time. Another alert will be generated at the end of the period indicating the number of the attack detected. Which IPS alert monitoring mechanism is configured?**
   - composite alert
   - atomic alert
   - correlation alert
   - **summary alert***

Alerts generated by an IPS should be monitored closely to ensure proper actions are taken against malicious attacks. IPS solutions incorporate two types of alerts, atomic alerts and summary alerts. Atomic alerts are generated every time a signature triggers. A summary alert is a single alert that indicates multiple occurrences of the same signature from the same source address or port. With a summary alter, the first detection of the attack triggers a normal alert. Subsequent detection of the same attack is counted until the end of the signature summary interval. When the length of time specified by the summary interval has elapsed, a summary alarm is sent, indicating the number of alarms that occurred during the time interval.

10. **Which statement is true about an atomic alert that is generated by an IPS?**
   - It is an alert that is used only when a logging attack has begun.
   - It is a single alert sent for multiple occurrences of the same signature.
   - **It is an alert that is generated every time a specific signature has been found.***
   - It is both a normal alarm and a summary alarm being sent simultaneously at set intervals.

The two main alert generation mechanisms for IDS/IPS devices are atomic and summary alerts. Atomic alerts are generated every time a signature triggers. With a summary alert, a single atomic alert is generated for the first detection of an attack. Then the duplicate alarms are counted, but not sent, for a specific time period. When it reaches the specified time period, an alert is sent that indicates the number of alarms that occurred during the time interval.

11. **Refer to the exhibit. Based on the configuration, which traffic will be examined by the IPS that is configured on router R1?**




```
R1(config)# ip ips name myips
R1(config)# ip ips name myips list 101
R1(config)# access-list 101 permit tcp 192.168.0.0 0.0.255.255 any eq http established
R1(config)# interface serial0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ip ips myips in
R1(config-if)# no shut
```

- traffic that is destined to LAN 1 and LAN 2
- return traffic from the web server
- traffic that is initiated from LAN 1 and LAN 2
- **no traffic will be inspected***
- http traffic that is initiated from LAN 1

Because the IPS inspection is configured on the S0/0/0 interface with inbound direction, but the ACL source address range is 192.168.0.0/16 and the traffic type is http established, there will be no traffic to match these criteria (note, there is no web server on LAN 1 or LAN 2). Hence no traffic inspection will take place.

12. **A network administrator suspects the default setting of the ip ips notify sdee command has caused performance degradation on the Cisco IOS IPS router. The network administrator enters the ip sdee events 50 command in an attempt to remedy the performance issues. What is the immediate effect of this command?**

- All events that were stored in the original buffer are saved, while a new buffer is created to store new events.
- **All events that were stored in the previous buffer are lost.***
- The newest 50 events from the original buffer are saved and all others are deleted.
- The oldest 50 events of the original buffer are deleted.

When sending IPS notification with SDEE format, the buffer on the router stores up to 200 events by default. If a smaller buffer is requested, all stored events are lost. If a larger buffer is requested, all stored events are saved. The default buffer can be altered with the ip sdee events command. All stored events are lost when Cisco SDEE notification is disabled. A new buffer is allocated when the notifications are re-enabled.

13. **True or False?**

A Cisco IDS does not affect the flow of traffic when it operates in promiscuous mode

- **true***
- false

In promiscuous mode, also known as passive mode, the flow of traffic is unaffected because the IDS sensor analyzes copies of traffic instead of actual forwarded packets.

14. **What is a required condition to enable IPS activity reporting using the SDEE format?**

- Create an IOS IPS configuration directory in flash.
- **Enable an HTTP or HTTPS service on the router.***
- Configure the signature category.
- Issue the ip ips notify log command.

To enable IPS activity reporting format using SDEE, the HTTP or HTTPS server must first be enabled on the router. If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot see the requests. The ip ips notify log command will send notification using syslog. The tasks of configuring the signature category and creating an IOS IPS configuration directory in flash are necessary to implement IOS IPS, but they are not directly associated with SDEE feature.

15. **Refer to the exhibit. Which statement best describes how incoming traffic on serial 0/0 is handled?**

```
Router# show running-config | begin ips
ip ips fail closed
ip ips name POLICY_101 list 100
<output omitted>
interface serial 0/0
  ip address 172.31.235.21 255.255.255.0
  ip ips POLICY_101 in
!
```

- Traffic that is coming from any source other than 172.31.235.0/24 will be scanned and reported.

- Traffic not matching ACL 100 will be dropped.
- Traffic not matching ACL 100 will be scanned and reported.
- Traffic that is sourced from 172.31.235.0/24 will be sent directly to its destination without being scanned or reported.
- **Traffic matching ACL 100 will be scanned and reported.***
- Traffic that is sourced from 172.31.235.0/24 will be scanned and reported.

From the configuration, ACL 100 is used to identify matching packets to be inspected. However, since the ACL 100 configuration is unknown (not displayed), the only conclusion we can draw for sure is that “Traffic matching ACL 100 will be scanned and reported.”

16. **Refer to the exhibit. Based on the IPS configuration provided, which conclusion can be drawn?**

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
```

- The signatures in all categories will be compiled into memory and used by the IPS.
- The signatures in all categories will be retired and not be used by the IPS.
- **Only the signatures in the ios_ips basic category will be compiled into memory and used by the IPS.***
- The signatures in the ios_ips basic category will be retired and the remaining signatures will be compiled into memory and used by the IPS.

The IPS signature in the all category is retired, which means no signatures are compiled into memory. The IPS signature ios_ips basic category is unretired (by the command retired false), resulting in the signatures in the ios_ips basic being compiled into RAM for traffic inspection.

17. **A network administrator is configuring an IOS IPS with the command**
R1(config)# ip ips signature-definition
Which configuration task can be achieved with this command?

- Retire or unretire the ios_ips basic signature category.
- **Retire or unretire an individual signature.***
- Retire or unretire the all signature category.

- Retire or unretire the all atomic signatures category.

The IOS command ip ips signature-definition is used to configure a specific signature, including retire/unretire and event action. To configure a signature category, the command ip ips signature-category is used.

18. **What are two disadvantages of using an IDS? (Choose two.)**
    - The IDS analyzes actual forwarded packets.
    - **The IDS does not stop malicious traffic.***
    - The IDS has no impact on traffic.
    - The IDS works offline using copies of network traffic.
    - **The IDS requires other devices to respond to attacks.***

The disadvantage of operating with mirrored traffic is that the IDS cannot stop malicious single-packet attacks from reaching the target before responding to the attack. Also, an IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack. An advantage of an IDS is that by working offline using mirrored traffic, it has no impact on traffic flow.

19. **What are two shared characteristics of the IDS and the IPS? (Choose two.)**
    - **Both use signatures to detect malicious traffic.***
    - Both analyze copies of network traffic.
    - Both have minimal impact on network performance.
    - Both rely on an additional network device to respond to malicious traffic.
    - **Both are deployed as sensors.***

Both the IDS and the IPS are deployed as sensors and use signatures to detect malicious traffic. The IDS analyzes copies of network traffic, which results in minimal impact on network performance. The IDS also relies on an IPS to stop malicious traffic.

20. **Refer to the exhibit. A network administrator enters the command on a Cisco IOS IPS router. What is the effect?**

```
Router(config)# ip ips notify
```

    - **Alert messages are sent in syslog format.***
    - Alert messages are sent in trace file format.
    - Alert messages are sent in Security Device Event Exchange (SDEE) format.
    - Alert messages are sent in event log format.

The ip ips notify command is used to set the IPS event notification. This command has two options, log and sdee. The log option is to specify that notifications are sent in syslog format.

The sdee option is to specify that notifications are sent in SDEE format. If no option is specified, by default, notifications are sent in syslog format.

21. **What is a disadvantage of network-based IPS as compared to host-based IPS?**
- Network-based IPS is less cost-effective.
- Network-based IPS should not be used with multiple operating systems.
- **Network-based IPS cannot examine encrypted traffic.***
- Network-based IPS does not detect lower level network events.

Network-based IPS devices are implemented as inline mode to actively monitor the traffic on networks. They can take immediate actions when security criteria match. One limitation of them is that they cannot monitor/inspect encrypted packets.

22. **An IPS sensor has detected the string confidential across multiple packets in a TCP session. Which type of signature trigger and signature type does this describe?**
- Trigger: Policy-based detection
  Type: Atomic signature
- Trigger: Policy-based detection
  Type: Composite signature
- Trigger: Anomaly-based detection
  Type: Atomic signature
- Trigger: Anomaly-based detection
  Type: Composite signature
- Trigger: Pattern-based detection
  Type: Atomic signature
- **Trigger: Pattern-based detection**
  Type: Composite signature*

Pattern-based detection (also called signature-based detection) searches for a specific pattern that can be textual, binary, or a series of function calls. It can be detected in a single packet (atomic) or in a packet sequence (composite).

23. **What are two drawbacks to using HIPS? (Choose two.)**
- With HIPS, the success or failure of an attack cannot be readily determined.
- **With HIPS, the network administrator must verify support for all the different operating systems used inthe network.***
- **HIPS has difficulty constructing an accurate network picture or coordinating events that occur across the entire network.***

- If the network traffic stream is encrypted, HIPS is unable to access unencrypted forms of the traffic.
- HIPS installations are vulnerable to fragmentation attacks or variable TTL attacks