



# Cisco

## Exam 500-280

### Securing Cisco Networks with Open Source Snort

Version: 6.0

[ Total Questions: 60 ]

**Question No : 1**

Which protocol operates below the network layer?

- A. UDP
- B. ICMP
- C. ARP
- D. DNS

**Answer: C**

**Question No : 2**

Which area is created between screening devices in an egress/ingress path for housing web, mail, or DNS servers?

- A. EMZ
- B. DMZ
- C. harbor
- D. inlet

**Answer: B**

**Question No : 3**

What does protocol normalization do?

- A. compares evaluated packets to normal, daily network-traffic patterns
- B. removes any protocol-induced or protocol-allowable ambiguities
- C. compares a packet to related traffic from the same session, to determine whether the packet is out of sequence
- D. removes application layer data, whether or not it carries protocol-induced anomalies, so that packet headers can be inspected more accurately for signs of abuse

**Answer: B**

**Question No : 4**

On which protocol does Snort focus to decode, process, and alert on suspicious network traffic?

- A. Apple talk
- B. TCP/IP
- C. IPX/SPX
- D. ICMP

**Answer: B**

**Question No : 5**

Which technique can an intruder use to try to evade detection by a Snort sensor?

- A. exceed the maximum number of fragments that a sensor can evaluate
- B. split the malicious payload over several fragments to mask the attack signature
- C. disable a sensor by exceeding the number of packets that it can fragment before forwarding
- D. send more packet fragments than the destination host can reassemble, to disable the host without regard to any intrusion-detection devices that might be on the network

**Answer: B**

**Question No : 6**

An IPS addresses evasion by implementing countermeasures. What is one such countermeasure?

- A. periodically reset statistical buckets to zero for memory utilization, maximization, and performance
- B. send packets to the origination host of a given communication session, to confirm or eliminate spoofing
- C. perform pattern and signature analysis against the entire packet, rather than against individual fragments
- D. automate scans of suspicious source IP addresses

**Answer: C**

**Question No : 7**

Which IPS placement option is the noisiest?

- A. inside the firewall
- B. outside the firewall
- C. inside the DMZ
- D. inside general user segments

**Answer: B**

**Question No : 8**

What is the purpose of using a span or monitor port on a switch?

- A. to aggregate traffic from multiple switch ports
- B. to tap data off network media
- C. to overcome problems that switches have in accurately reproducing desired traffic
- D. to limit the amount of traffic that passes through the switch

**Answer: A**

**Question No : 9**

Which item examines packets for malformation, anomalies, and protocol compliance and gathers and presents packets in one consistent fashion?

- A. Sniffer
- B. preprocessors
- C. detection engine
- D. output and alerting module

**Answer: B**

**Question No : 10**

Which component is one of the four primary components of Snort?

- A. ACL
- B. postprocessor
- C. iptables
- D. output and alerting

**Answer: D**

**Question No : 11**

Which engine or module presents alert and log data in the format that you specify?

- A. tap
- B. sniffing
- C. detection
- D. output

**Answer: D**

**Question No : 12**

Other than intrusion sensing, which other function set can Snort perform?

- A. packet sniffing and disassembly
- B. packet logging and alerting
- C.
- D. packet sniffing and logging

**Answer: D**

**Question No : 13**

Which output is in a lightweight, binary form?

- A. unified2
- B. PCAP
- C. SNMP
- D. CSV

**Answer: A**

**Question No : 14**

What does packet sniffing do?

- A. isolates datagrams into like groups
- B. reads datagrams directly off the wire
- C. transmits datagrams over a wireless network
- D. rebuilds datagram streams

**Answer: B**

**Question No : 15**

When building a platform for a Snort installation, which set of components is a major security concern?

- A. IP address, mask, and gateway settings
- B. host naming conventions
- C. URL feed vendors
- D. default accounts and settings

**Answer: D**

**Question No : 16**

In the IP addressing scheme of your organization, each subnet consists of 4096 hosts, and the beginning of the addressing scheme is 172.16.0.0. Your remote office is allocated the range of addresses from the first subnet. What are the CIDR notation, network address, broadcast address, and valid IP address in your assigned range?

- A. 172.16.0.0/24, 172.16.0.0, 172.16.8.255, 172.16.0.51
- B. 172.16.0.0/20, 172.16.0.0, 172.16.15.255, 172.16.8.252
- C. 172.16.0.0/16, 172.16.0.0, 172.16.32.255, 172.16.22.4
- D. 172.16.0.0/12, 172.16.0.0, 172.16.64.255, 172.16.52.112

### Microsoft Exams List

|                                     |                                     |                                     |                                      |
|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------------------|
| <a href="#">70-246 Dump PDF VCE</a> | <a href="#">70-485 Dump PDF VCE</a> | <a href="#">70-742 Dump PDF VCE</a> | <a href="#">98-366 Dump PDF VCE</a>  |
| <a href="#">70-247 Dump PDF VCE</a> | <a href="#">70-486 Dump PDF VCE</a> | <a href="#">70-743 Dump PDF VCE</a> | <a href="#">98-367 Dump PDF VCE</a>  |
| <a href="#">70-331 Dump PDF VCE</a> | <a href="#">70-487 Dump PDF VCE</a> | <a href="#">70-744 Dump PDF VCE</a> | <a href="#">98-368 Dump PDF VCE</a>  |
| <a href="#">70-332 Dump PDF VCE</a> | <a href="#">70-488 Dump PDF VCE</a> | <a href="#">70-761 Dump PDF VCE</a> | <a href="#">98-369 Dump PDF VCE</a>  |
| <a href="#">70-333 Dump PDF VCE</a> | <a href="#">70-489 Dump PDF VCE</a> | <a href="#">70-762 Dump PDF VCE</a> | <a href="#">98-372 Dump PDF VCE</a>  |
| <a href="#">70-334 Dump PDF VCE</a> | <a href="#">70-490 Dump PDF VCE</a> | <a href="#">70-765 Dump PDF VCE</a> | <a href="#">98-373 Dump PDF VCE</a>  |
| <a href="#">70-339 Dump PDF VCE</a> | <a href="#">70-491 Dump PDF VCE</a> | <a href="#">70-768 Dump PDF VCE</a> | <a href="#">98-374 Dump PDF VCE</a>  |
| <a href="#">70-341 Dump PDF VCE</a> | <a href="#">70-492 Dump PDF VCE</a> | <a href="#">70-980 Dump PDF VCE</a> | <a href="#">98-375 Dump PDF VCE</a>  |
| <a href="#">70-342 Dump PDF VCE</a> | <a href="#">70-494 Dump PDF VCE</a> | <a href="#">70-981 Dump PDF VCE</a> | <a href="#">98-379 Dump PDF VCE</a>  |
| <a href="#">70-345 Dump PDF VCE</a> | <a href="#">70-496 Dump PDF VCE</a> | <a href="#">70-982 Dump PDF VCE</a> | <a href="#">MB2-700 Dump PDF VCE</a> |
| <a href="#">70-346 Dump PDF VCE</a> | <a href="#">70-497 Dump PDF VCE</a> | <a href="#">74-343 Dump PDF VCE</a> | <a href="#">MB2-701 Dump PDF VCE</a> |
| <a href="#">70-347 Dump PDF VCE</a> | <a href="#">70-498 Dump PDF VCE</a> | <a href="#">74-344 Dump PDF VCE</a> | <a href="#">MB2-702 Dump PDF VCE</a> |
| <a href="#">70-348 Dump PDF VCE</a> | <a href="#">70-499 Dump PDF VCE</a> | <a href="#">74-409 Dump PDF VCE</a> | <a href="#">MB2-703 Dump PDF VCE</a> |
| <a href="#">70-354 Dump PDF VCE</a> | <a href="#">70-517 Dump PDF VCE</a> | <a href="#">74-678 Dump PDF VCE</a> | <a href="#">MB2-704 Dump PDF VCE</a> |
| <a href="#">70-383 Dump PDF VCE</a> | <a href="#">70-532 Dump PDF VCE</a> | <a href="#">74-697 Dump PDF VCE</a> | <a href="#">MB2-707 Dump PDF VCE</a> |
| <a href="#">70-384 Dump PDF VCE</a> | <a href="#">70-533 Dump PDF VCE</a> | <a href="#">77-420 Dump PDF VCE</a> | <a href="#">MB2-710 Dump PDF VCE</a> |
| <a href="#">70-385 Dump PDF VCE</a> | <a href="#">70-534 Dump PDF VCE</a> | <a href="#">77-427 Dump PDF VCE</a> | <a href="#">MB2-711 Dump PDF VCE</a> |
| <a href="#">70-410 Dump PDF VCE</a> | <a href="#">70-640 Dump PDF VCE</a> | <a href="#">77-600 Dump PDF VCE</a> | <a href="#">MB2-712 Dump PDF VCE</a> |
| <a href="#">70-411 Dump PDF VCE</a> | <a href="#">70-642 Dump PDF VCE</a> | <a href="#">77-601 Dump PDF VCE</a> | <a href="#">MB2-713 Dump PDF VCE</a> |
| <a href="#">70-412 Dump PDF VCE</a> | <a href="#">70-646 Dump PDF VCE</a> | <a href="#">77-602 Dump PDF VCE</a> | <a href="#">MB2-714 Dump PDF VCE</a> |
| <a href="#">70-413 Dump PDF VCE</a> | <a href="#">70-673 Dump PDF VCE</a> | <a href="#">77-603 Dump PDF VCE</a> | <a href="#">MB2-715 Dump PDF VCE</a> |
| <a href="#">70-414 Dump PDF VCE</a> | <a href="#">70-680 Dump PDF VCE</a> | <a href="#">77-604 Dump PDF VCE</a> | <a href="#">MB2-716 Dump PDF VCE</a> |
| <a href="#">70-417 Dump PDF VCE</a> | <a href="#">70-681 Dump PDF VCE</a> | <a href="#">77-605 Dump PDF VCE</a> | <a href="#">MB2-717 Dump PDF VCE</a> |
| <a href="#">70-461 Dump PDF VCE</a> | <a href="#">70-682 Dump PDF VCE</a> | <a href="#">77-881 Dump PDF VCE</a> | <a href="#">MB2-718 Dump PDF VCE</a> |
| <a href="#">70-462 Dump PDF VCE</a> | <a href="#">70-684 Dump PDF VCE</a> | <a href="#">77-882 Dump PDF VCE</a> | <a href="#">MB5-705 Dump PDF VCE</a> |
| <a href="#">70-463 Dump PDF VCE</a> | <a href="#">70-685 Dump PDF VCE</a> | <a href="#">77-883 Dump PDF VCE</a> | <a href="#">MB6-700 Dump PDF VCE</a> |
| <a href="#">70-464 Dump PDF VCE</a> | <a href="#">70-686 Dump PDF VCE</a> | <a href="#">77-884 Dump PDF VCE</a> | <a href="#">MB6-701 Dump PDF VCE</a> |
| <a href="#">70-465 Dump PDF VCE</a> | <a href="#">70-687 Dump PDF VCE</a> | <a href="#">77-885 Dump PDF VCE</a> | <a href="#">MB6-702 Dump PDF VCE</a> |
| <a href="#">70-466 Dump PDF VCE</a> | <a href="#">70-688 Dump PDF VCE</a> | <a href="#">77-886 Dump PDF VCE</a> | <a href="#">MB6-703 Dump PDF VCE</a> |
| <a href="#">70-467 Dump PDF VCE</a> | <a href="#">70-689 Dump PDF VCE</a> | <a href="#">77-887 Dump PDF VCE</a> | <a href="#">MB6-704 Dump PDF VCE</a> |
| <a href="#">70-469 Dump PDF VCE</a> | <a href="#">70-692 Dump PDF VCE</a> | <a href="#">77-888 Dump PDF VCE</a> | <a href="#">MB6-705 Dump PDF VCE</a> |
| <a href="#">70-470 Dump PDF VCE</a> | <a href="#">70-695 Dump PDF VCE</a> | <a href="#">77-891 Dump PDF VCE</a> | <a href="#">MB6-884 Dump PDF VCE</a> |
| <a href="#">70-473 Dump PDF VCE</a> | <a href="#">70-696 Dump PDF VCE</a> | <a href="#">98-349 Dump PDF VCE</a> | <a href="#">MB6-885 Dump PDF VCE</a> |
| <a href="#">70-480 Dump PDF VCE</a> | <a href="#">70-697 Dump PDF VCE</a> | <a href="#">98-361 Dump PDF VCE</a> | <a href="#">MB6-886 Dump PDF VCE</a> |
| <a href="#">70-481 Dump PDF VCE</a> | <a href="#">70-698 Dump PDF VCE</a> | <a href="#">98-362 Dump PDF VCE</a> | <a href="#">MB6-889 Dump PDF VCE</a> |
| <a href="#">70-482 Dump PDF VCE</a> | <a href="#">70-734 Dump PDF VCE</a> | <a href="#">98-363 Dump PDF VCE</a> | <a href="#">MB6-890 Dump PDF VCE</a> |
| <a href="#">70-483 Dump PDF VCE</a> | <a href="#">70-740 Dump PDF VCE</a> | <a href="#">98-364 Dump PDF VCE</a> | <a href="#">MB6-892 Dump PDF VCE</a> |
| <a href="#">70-484 Dump PDF VCE</a> | <a href="#">70-741 Dump PDF VCE</a> | <a href="#">98-365 Dump PDF VCE</a> | <a href="#">MB6-893 Dump PDF VCE</a> |

### Cisco Exams List

|                                      |                                      |                                      |                                      |
|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|
| <a href="#">010-151 Dump PDF VCE</a> | <a href="#">350-018 Dump PDF VCE</a> | <a href="#">642-737 Dump PDF VCE</a> | <a href="#">650-667 Dump PDF VCE</a> |
| <a href="#">100-105 Dump PDF VCE</a> | <a href="#">352-001 Dump PDF VCE</a> | <a href="#">642-742 Dump PDF VCE</a> | <a href="#">650-669 Dump PDF VCE</a> |
| <a href="#">200-001 Dump PDF VCE</a> | <a href="#">400-051 Dump PDF VCE</a> | <a href="#">642-883 Dump PDF VCE</a> | <a href="#">650-752 Dump PDF VCE</a> |
| <a href="#">200-105 Dump PDF VCE</a> | <a href="#">400-101 Dump PDF VCE</a> | <a href="#">642-885 Dump PDF VCE</a> | <a href="#">650-756 Dump PDF VCE</a> |
| <a href="#">200-120 Dump PDF VCE</a> | <a href="#">400-151 Dump PDF VCE</a> | <a href="#">642-887 Dump PDF VCE</a> | <a href="#">650-968 Dump PDF VCE</a> |
| <a href="#">200-125 Dump PDF VCE</a> | <a href="#">400-201 Dump PDF VCE</a> | <a href="#">642-889 Dump PDF VCE</a> | <a href="#">700-001 Dump PDF VCE</a> |
| <a href="#">200-150 Dump PDF VCE</a> | <a href="#">400-251 Dump PDF VCE</a> | <a href="#">642-980 Dump PDF VCE</a> | <a href="#">700-037 Dump PDF VCE</a> |
| <a href="#">200-155 Dump PDF VCE</a> | <a href="#">400-351 Dump PDF VCE</a> | <a href="#">642-996 Dump PDF VCE</a> | <a href="#">700-038 Dump PDF VCE</a> |
| <a href="#">200-310 Dump PDF VCE</a> | <a href="#">500-006 Dump PDF VCE</a> | <a href="#">642-997 Dump PDF VCE</a> | <a href="#">700-039 Dump PDF VCE</a> |
| <a href="#">200-355 Dump PDF VCE</a> | <a href="#">500-007 Dump PDF VCE</a> | <a href="#">642-998 Dump PDF VCE</a> | <a href="#">700-101 Dump PDF VCE</a> |
| <a href="#">200-401 Dump PDF VCE</a> | <a href="#">500-051 Dump PDF VCE</a> | <a href="#">642-999 Dump PDF VCE</a> | <a href="#">700-104 Dump PDF VCE</a> |
| <a href="#">200-601 Dump PDF VCE</a> | <a href="#">500-052 Dump PDF VCE</a> | <a href="#">644-066 Dump PDF VCE</a> | <a href="#">700-201 Dump PDF VCE</a> |
| <a href="#">210-060 Dump PDF VCE</a> | <a href="#">500-170 Dump PDF VCE</a> | <a href="#">644-068 Dump PDF VCE</a> | <a href="#">700-205 Dump PDF VCE</a> |
| <a href="#">210-065 Dump PDF VCE</a> | <a href="#">500-201 Dump PDF VCE</a> | <a href="#">644-906 Dump PDF VCE</a> | <a href="#">700-260 Dump PDF VCE</a> |
| <a href="#">210-250 Dump PDF VCE</a> | <a href="#">500-202 Dump PDF VCE</a> | <a href="#">646-048 Dump PDF VCE</a> | <a href="#">700-270 Dump PDF VCE</a> |
| <a href="#">210-255 Dump PDF VCE</a> | <a href="#">500-254 Dump PDF VCE</a> | <a href="#">646-365 Dump PDF VCE</a> | <a href="#">700-280 Dump PDF VCE</a> |
| <a href="#">210-260 Dump PDF VCE</a> | <a href="#">500-258 Dump PDF VCE</a> | <a href="#">646-580 Dump PDF VCE</a> | <a href="#">700-281 Dump PDF VCE</a> |
| <a href="#">210-451 Dump PDF VCE</a> | <a href="#">500-260 Dump PDF VCE</a> | <a href="#">646-671 Dump PDF VCE</a> | <a href="#">700-295 Dump PDF VCE</a> |
| <a href="#">210-455 Dump PDF VCE</a> | <a href="#">500-265 Dump PDF VCE</a> | <a href="#">646-985 Dump PDF VCE</a> | <a href="#">700-501 Dump PDF VCE</a> |
| <a href="#">300-070 Dump PDF VCE</a> | <a href="#">500-275 Dump PDF VCE</a> | <a href="#">648-232 Dump PDF VCE</a> | <a href="#">700-505 Dump PDF VCE</a> |
| <a href="#">300-075 Dump PDF VCE</a> | <a href="#">500-280 Dump PDF VCE</a> | <a href="#">648-238 Dump PDF VCE</a> | <a href="#">700-601 Dump PDF VCE</a> |
| <a href="#">300-080 Dump PDF VCE</a> | <a href="#">500-285 Dump PDF VCE</a> | <a href="#">648-244 Dump PDF VCE</a> | <a href="#">700-602 Dump PDF VCE</a> |
| <a href="#">300-085 Dump PDF VCE</a> | <a href="#">500-290 Dump PDF VCE</a> | <a href="#">648-247 Dump PDF VCE</a> | <a href="#">700-603 Dump PDF VCE</a> |
| <a href="#">300-101 Dump PDF VCE</a> | <a href="#">500-801 Dump PDF VCE</a> | <a href="#">648-375 Dump PDF VCE</a> | <a href="#">700-701 Dump PDF VCE</a> |
| <a href="#">300-115 Dump PDF VCE</a> | <a href="#">600-199 Dump PDF VCE</a> | <a href="#">648-385 Dump PDF VCE</a> | <a href="#">700-702 Dump PDF VCE</a> |
| <a href="#">300-135 Dump PDF VCE</a> | <a href="#">600-210 Dump PDF VCE</a> | <a href="#">650-032 Dump PDF VCE</a> | <a href="#">700-703 Dump PDF VCE</a> |
| <a href="#">300-160 Dump PDF VCE</a> | <a href="#">600-211 Dump PDF VCE</a> | <a href="#">650-042 Dump PDF VCE</a> | <a href="#">700-801 Dump PDF VCE</a> |
| <a href="#">300-165 Dump PDF VCE</a> | <a href="#">600-212 Dump PDF VCE</a> | <a href="#">650-059 Dump PDF VCE</a> | <a href="#">700-802 Dump PDF VCE</a> |
| <a href="#">300-180 Dump PDF VCE</a> | <a href="#">600-455 Dump PDF VCE</a> | <a href="#">650-082 Dump PDF VCE</a> | <a href="#">700-803 Dump PDF VCE</a> |
| <a href="#">300-206 Dump PDF VCE</a> | <a href="#">600-460 Dump PDF VCE</a> | <a href="#">650-127 Dump PDF VCE</a> | <a href="#">810-403 Dump PDF VCE</a> |
| <a href="#">300-207 Dump PDF VCE</a> | <a href="#">600-501 Dump PDF VCE</a> | <a href="#">650-128 Dump PDF VCE</a> | <a href="#">820-424 Dump PDF VCE</a> |
| <a href="#">300-208 Dump PDF VCE</a> | <a href="#">600-502 Dump PDF VCE</a> | <a href="#">650-148 Dump PDF VCE</a> | <a href="#">840-425 Dump PDF VCE</a> |
| <a href="#">300-209 Dump PDF VCE</a> | <a href="#">600-503 Dump PDF VCE</a> | <a href="#">650-159 Dump PDF VCE</a> |                                      |
| <a href="#">300-210 Dump PDF VCE</a> | <a href="#">600-504 Dump PDF VCE</a> | <a href="#">650-281 Dump PDF VCE</a> |                                      |
| <a href="#">300-320 Dump PDF VCE</a> | <a href="#">640-692 Dump PDF VCE</a> | <a href="#">650-393 Dump PDF VCE</a> |                                      |
| <a href="#">300-360 Dump PDF VCE</a> | <a href="#">640-875 Dump PDF VCE</a> | <a href="#">650-472 Dump PDF VCE</a> |                                      |
| <a href="#">300-365 Dump PDF VCE</a> | <a href="#">640-878 Dump PDF VCE</a> | <a href="#">650-474 Dump PDF VCE</a> |                                      |
| <a href="#">300-370 Dump PDF VCE</a> | <a href="#">640-911 Dump PDF VCE</a> | <a href="#">650-575 Dump PDF VCE</a> |                                      |
| <a href="#">300-375 Dump PDF VCE</a> | <a href="#">640-916 Dump PDF VCE</a> | <a href="#">650-621 Dump PDF VCE</a> |                                      |
| <a href="#">300-465 Dump PDF VCE</a> | <a href="#">642-035 Dump PDF VCE</a> | <a href="#">650-663 Dump PDF VCE</a> |                                      |
| <a href="#">300-470 Dump PDF VCE</a> | <a href="#">642-732 Dump PDF VCE</a> | <a href="#">650-665 Dump PDF VCE</a> |                                      |
| <a href="#">300-475 Dump PDF VCE</a> | <a href="#">642-747 Dump PDF VCE</a> | <a href="#">650-754 Dump PDF VCE</a> |                                      |



## HOT EXAMS

### Cisco

[100-105 Dumps VCE PDF](#)  
[200-105 Dumps VCE PDF](#)  
[300-101 Dumps VCE PDF](#)  
[300-115 Dumps VCE PDF](#)  
[300-135 Dumps VCE PDF](#)  
[300-320 Dumps VCE PDF](#)  
[400-101 Dumps VCE PDF](#)  
[640-911 Dumps VCE PDF](#)  
[640-916 Dumps VCE PDF](#)

### Microsoft

[70-410 Dumps VCE PDF](#)  
[70-411 Dumps VCE PDF](#)  
[70-412 Dumps VCE PDF](#)  
[70-413 Dumps VCE PDF](#)  
[70-414 Dumps VCE PDF](#)  
[70-417 Dumps VCE PDF](#)  
[70-461 Dumps VCE PDF](#)  
[70-462 Dumps VCE PDF](#)  
[70-463 Dumps VCE PDF](#)  
[70-464 Dumps VCE PDF](#)  
[70-465 Dumps VCE PDF](#)  
[70-480 Dumps VCE PDF](#)  
[70-483 Dumps VCE PDF](#)  
[70-486 Dumps VCE PDF](#)  
[70-487 Dumps VCE PDF](#)

### CompTIA

[220-901 Dumps VCE PDF](#)  
[220-902 Dumps VCE PDF](#)  
[N10-006 Dumps VCE PDF](#)  
[SY0-401 Dumps VCE PDF](#)