

ITCertMagic

ITCertMagic

HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

CART (0)



Try **PDF Demo** before you buy

28 Top Certifications

Apr

- ▶ HP CSE ▶ Avaya Specialist
- ▶ ACE InDesign ▶ LPIC Level1
- ▶ Apple Certified Pro ▶ VCP6-CMA
- ▶ JNCDA ▶ Aruba Certification ▶ CCA XP
- ▶ ICND1 ▶ RCSP ▶ GAQM LCP
- ▶ JNCDS-SEC ▶ Fireware Essentials
- ▶ Oracle Spatial 11g


28 Top Vendors

Apr

- ▶ ISM ▶ HRCI
- ▶ Palo Alto Networks ▶ NSCA
- ▶ SUN ▶ ISQI ▶ Huawei
- ▶ American College ▶ IIA ▶ ARM
- ▶ Pegasystems ▶ OMG ▶ Simens ▶ GRE
- ▶ HAAD ▶ PCI ▶ BBPSD ▶ SCO
- ▶ SugarCRM ▶ Logical Operations ▶ IIBA
- ▶ Altiris ▶ Alfresco ▶ AMA ▶ Informatca

What Client's Say

“ There are some less than 8 new questions, so this 70-695 dump is still mostly valid. Wrote the exams today and passed. ”

 **Timothy**
★★★★★

<http://www.itcertmagic.com/>

Pass-Guaranteed Certification Exam Questions | Exam Dumps - ITCertMagic

Exam : **600-199**

Title : **Securing Cisco Networks with
Threat Detection and Analysis**

Vendor : **Cisco**

Version : **DEMO**

NO.1 Which two tools are used to help with traffic identification? (Choose two.)

- A. network sniffer
- B. ping
- C. traceroute
- D. route table
- E. NetFlow
- F. DHCP

Answer: A,E

NO.2 Which step should be taken first when a server on a network is compromised?

- A. Refer to the company security policy.
- B. Email all server administrators.
- C. Determine which server has been compromised.
- D. Find the serial number of the server.

Answer: A

NO.3 Refer to the exhibit.

```
15:59:06.480292 IP 10.10.10.10.http > 192.168.10.2.58320: Flags [.], seq 82080, ack 1, win 16416, options [nop,nop,TS val 1991638787 ecr 459929244], length 1368
15:59:06.480375 IP 10.10.10.10.http > 192.168.10.2.58320: Flags [.], seq XXXXX, ack 1, win 16416, options [nop,nop,TS val 1991638787 ecr 459929244], length 1368
```

In the tcpdump output, what is the sequence number that is represented by XXXXX?

- A. 82080
- B. 82081
- C. 83448
- D. 83449
- E. 98496
- F. 98497

Answer: C

NO.4 When an IDS generates an alert for a correctly detected network attack, what is this event called?

- A. false positive
- B. true negative
- C. true positive
- D. false negative

Answer: C

NO.5 What are four steps to manage incident response handling? (Choose four.)

- A. preparation
- B. qualify
- C. identification
- D. who
- E. containment
- F. recovery
- G. eradication
- H. lessons learned

Answer: A,C,E,H