



[CompTIA BR0-001](#)

Exam Name: *CompTIA Bridge Exam - Security+*

Q & A : 73 Q&As

Pdf Demo

Quality and Value for the BR0-001 Exam

[Just4Exams Practice Exams](#) for CompTIA Security BR0-001 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

100% Guarantee to Pass Your BR0-001 Exam

If you do not pass the Security BR0-001 exam on your first attempt using our Just4Exams **BR0-001 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

Downloadable, Interactive BR0-001 Testing engines and PDF Version

Our Exam Preparation Material provides you everything you will need to take a [Security certification](#) examination. Details are researched and produced by [CompTIA Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

Free BR0-001 Exams:

This is demo only, this pdf do not include the questions and answers picture

Exam : CompTIA BR0-001

Title : CompTIA Bridge Exam - Security+

1. An administrator wants to proactively collect information on attackers and their attempted methods of gaining access to the internal network. Which of the following would allow the administrator to do this?

- A. NIPS
- B. Honeypot
- C. DMZ
- D. NIDS

Answer: B

2. Which of the following technologies can be used as a means to isolate a host OS from some types of security threats?

- A. Intrusion detection
- B. Virtualization
- C. Kiting
- D. Cloning

Answer: B

3. Which of the following encryption methods is often used along with L2TP?

- A. S/MIME
- B. SSH
- C. 3DES
- D. IPSec

Answer: D

4. Taking into account personal safety, which of the following types of fire suppression substances would BEST prevent damage to electronic equipment?

- A. Foam
- B. CO2
- C. Halon
- D. Water

Answer: B

5. Which of the following would an attacker use to footprint a system?

- A. RADIUS
- B. Password cracker
- C. Port scanner
- D. Man-in-the-middle attack

Answer: C

6. If a user attempts to go to a website and notices the URL has changed, which of the following attacks is MOST likely the cause?

- A. DLL injection
- B. DDoS attack
- C. DNS poisoning
- D. ARP poisoning

Answer: C

7. Which of the following is a reason to implement security logging on a DNS server?

- A. To monitor unauthorized zone transfers
- B. To measure the DNS server performance
- C. To perform penetration testing on the DNS server
- D. To control unauthorized DNS DoS

Answer: A

8. Which of the following tools will allow the technician to find all open ports on the network?

- A. Performance monitor
- B. Protocol analyzer
- C. Router ACL
- D. Network scanner

Answer: D

9. Which of the following describes the process of securely removing information from media (e.g. hard drive) for future use?

- A. Reformatting
- B. Destruction
- C. Sanitization
- D. Deleting

Answer: C

10. An executive uses PKI to encrypt sensitive emails sent to an assistant. In addition to encrypting the body of the email, the executive wishes to encrypt the signature so that the assistant can verify that the email actually came from the executive. Which of the following asymmetric keys should the executive use to encrypt the signature?

- A. Public
- B. Private

C.Shared
D.Hash
Answer: B

11. Which of the following security policies is BEST to use when trying to mitigate the risks involved with allowing a user to access company email via their cell phone?

- A.The cell phone should require a password after a set period of inactivity.
- B.The cell phone should only be used for company related emails.
- C.The cell phone data should be encrypted according to NIST standards.
- D.The cell phone should have data connection abilities disabled.

Answer: A

12. Which of the following describes a static NAT?

- A.A static NAT uses a one to many mapping.
- B.A static NAT uses a many to one mapping.
- C.A static NAT uses a many to many mapping.
- D.A static NAT uses a one to one mapping.

Answer: D

13. Which of the following is the LEAST intrusive way of checking the environment for known software flaws?

- A.Protocol analyzer
- B.Vulnerability scanner
- C.Port scanner
- D.Penetration test

Answer: B

14. Which of the following specifies a set of consistent requirements for a workstation or server?

- A.Vulnerability assessment
- B.Imaging software
- C.Patch management
- D.Configuration baseline

Answer: D

15. Which of the following requires an update to the baseline after installing new software on a machine?

- A.Signature-based NIPS
- B.Signature-based NIDS
- C.Honeypot
- D.Behavior-based HIDS

Answer: D

More [BR0-001 Braindumps](#) Information

Related BR0-001 Exams

SY0-201	sy0-101	BR0-001	BR0-002	JK0-010
JK0-015				

Other CompTIA Exams

PD0-001	JK0-013	JK0-015	HT0-101	220-612
JK0-014	JK0-016	JK0-601	FC0-U11	SY0-201
FC0-U21	BR0-003	TK0-201	CT0-101	220-301
HT0-102	sk0-002	PK1-003	220-601	220-702