Braindump2go Guarantee All Exams 100% Pass One Time!

- Vendor: CompTIA
- Exam Code: SY0-501
- Exam Name: CompTIA Security+ Certification Exam
- New Updated Questions from Braindump2go (Updated in June/2020)

Visit Braindump2go and Download Full Version SY0-501 Exam Dumps

QUESTION 907
After successfully breaking into several networks and infecting multiple machines with malware. hackers contact the network owners. demanding payment to remove the infection and decrypt files. The hackers threaten to publicly release information about the breach if they are not paid. Which of the following BEST describes these attackers?

A. Gray hat hackers
B. Organized crime
C. Insiders
D. Hacktivists

Answer: C

QUESTION 908
A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine.
B. Open the file and run it.
C. Create a secure baseline of the system state.
D. Hardon the machine

Answer: C

QUESTION 909
A company has a team of penetration testers, This team has located a file on the company file server that they believe contains clear text usernames ** by a hash. Which of the following tools should the penetration testers use to learn more about the content of this file?

A. Exploitation framework
B. Vulnerability scanner
C. Netcat
D. Password cracker

Answer: C

QUESTION 910
A security engineer is looking to purchase a fingerprint scanner to improve the security of a datacenter. Which of the following scanner characteristics is the MOST critical to successful implementation?

MB-310 Exam Dumps MB-310 Exam Questions MB-310 PDF Dumps MB-310 VCE Dumps https://www.braindump2go.com/sy0-501.html

A. Low false rejection rate
B. High false rejection rate
C. High false acceptance rate
D. Low crossover error rate

Answer: D

QUESTION 911
Which of the following attacks is unique in that no data is collected from the victim?

A. DoS
B. Phishing
C. MITM
D. Evil twin

Answer: A

QUESTION 912
A security analyst runs the following command:
netstat -anb

Proto	Local Address	Foreign Address	State	PID	Application
TCP	192.168.13.14:5169	10.1.1.5:80	ESTABLISHED	663	iexplore.exe
TCP	192.168.13.14:2190	10.1.1.5:443	ESTABLISHED	441	chrome.exe
TCP	192.168.13.14:75	10.1.1.5:1456	LISTENING	991	notepad.exe
UDP	192.168.13.14:4180	*:*		3	

Based on the above information, with which of the following types of malware is the server MOST likely infected?

A. Worm
B. RAT
C. Keylogger
D. Adware

Answer: A

QUESTION 913
Which of the following could an attacker use to overwrite instruction pointers in order to execute malicious code?

A. Memory leak
B. SQL injection
C. Resource exhaustion
D. Buffer overflow

Answer: D

QUESTION 914
A security team has downloaded a public database of the largest collection of password dumps on the Internet. This collection contains the cleartext credentials of every major breach for the last four years. The security team pulls and compares users' credentials to the database and discovers that more than 30% of the users were still using passwords discovered in this list. Which of the following would be the BEST combination to reduce the risks discovered?

A. Password length, password encryption, password complexity
B. Password complexity, least privilege, password reuse
C. Password reuse, password complexity, password expiration

D. Group policy, password history, password encryption

Answer: A

QUESTION 915
A user wants to send a confidential message to a customer to ensure unauthorized users cannot access the information. Which of the following can be used to ensure the security of the document while in transit and at rest?

A. BCRYPT
B. PGP
C. FTPS
D. S/MIME

Answer: B

QUESTION 916
A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords
B. Use SSH for remote access
C. Configure SNMPv2 for device management
D. Use TFTP to copy device configuration

Answer: B

QUESTION 917
An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

Answer: B

QUESTION 918
A security administrator is investigating a possible account compromise. The administrator logs onto a desktop computer, executes the command notepad.exe `c:\Temp\qkakforlkgfkja.log`, and reviews the following:
`Lee,\rI have completed the task that was assigned to me\rrespectfully\rJohn\r https://www.portal.com\rjohnuser\rilovemycat2`
Given the above output, which of the following is the MOST likely cause of this compromise?

A. Virus
B. Worm
C. Rootkit
D. Keylogger

Answer: D