[April-2021Braindump2go SY0-501 1366 SY0-501 Dumps VCE Free Share[Q1333-Q1366

April/2021 Latest Braindump2go SY0-501 Exam Dumps with PDF and VCE Free Updated Today! Following are some new SY0-501 Real Exam Questions!QUESTION 1333A technician is implementing 802.1X with dynamic VLAN assignment based on a user Active Directory group membership. Which of the following configurations supports the VLAN definitions?A.   RADIUS attributeB.   SAML tagC.   LDAP pathD.   Shibboleth IdPAnswer: AQUESTION 1334Which of the following agreement types is a non-contractual agreement between two or more parties and outlines each party's requirements and responsibilities?A.   BPAB.   SLAC.   MOUD.   ISAAnswer: CQUESTION 1335A technician wants to implement PKI-based authentication on an enterprise wireless network. Which of the following should the technician configure to enforce the use of client-side certificates?A.   802.1X with PEAPB.   WPA2-PSKC.   EAP-TLSD.   RADIUS FederationAnswer: CQUESTION 1336A company has forbidden the use of external media within its headquarters location. A security analyst is working on adding additional repositories to a server in the environment when the analyst notices some odd processes running on the system. The analyst runs a command and sees the following:

```
$ history
    ifconfig -a
    netstat -n
    pskill 1788
    pskill 914
    mkdir /tmp/1
    mount ... ...
    cp /tmp/1/* ~/1/
    umount /tmp/1
    ls -al 1/1/
    apt-get update
    apt-get upgrade
    clear
```

Given this output, which of the following security issues has been discovered?A.   A misconfigured HIDSB.   A malware installationC.   A policy violationD.   The activation of a TrojanAnswer: BQUESTION 1337During certain vulnerability scanning scenarios, it is possible for the target system to react in unexpected ways. This type of scenario is MOST commonly known as:A.   intrusive testingB.   a buffer overflowC.   a race conditionD.   active reconnaissanceAnswer: AQUESTION 1338An organization prefers to apply account permissions to groups and not individual users, but allows for exceptions that are justified. Some systems require a machine-to-machine data exchange and an associated account to perform this data exchange. One particular system has data in a folder that must be modified by another system. No user requires access to this folder; only the other system needs access to this folder. Which of the following is the BEST account management practice?A.   Create a service account and apply the necessary permissions directly to the service account itselfB.   Create a service account group, place the service account in the group, and apply the permissions on the groupC.   Create a guest account and restrict the permissions to only the folder with the dataD.   Create a generic account that will only be used for accessing the folder, but disable the account until it is needed for the data exchangeE.   Create a shared account that administrators can use to exchange the data, but audit the shared account activityAnswer: AQUESTION 1339A user attempts to send an email to an external domain and quickly receives a bounce-back message. The user then contacts the help desk stating the message is important and needs to be delivered immediately. While digging through the email logs, a systems administrator finds the email and bounce- back details:Your email has been rejected because it appears to contain SSN information. Sending SSN information via email to external recipients violates company policy. Which of the following technologies successfully stopped the email from being sent?A.   DLPB.   UTMC.   WAFD.

DEPAnswer: AQUESTION 1340Which of the following controls does a mantrap BEST represent?A.   DeterrentB.   DetectiveC.   PhysicalD.   CorrectiveAnswer: CQUESTION 1341A security administrator has created a new group policy object that utilizes the trusted platform module to compute a hash of system files and compare the value to a known-good value. Which of the following security concepts is this an example of?A.   Integrity measurementB.   Secure baselineC.   SandboxingD.   Immutable systemsAnswer: AQUESTION 1342A network administrator wants to gather information on the security of the network servers in the DMZ. The administrator runs the following command:Telnet www.example.com 80Which of the following actions is the administrator performing?A.   Grabbing the web server bannerB.   Logging into the web serverC.   Harvesting cleartext credentialsD.   Accessing the web server management consoleAnswer: AQUESTION 1343Which of the following should be implemented to stop an attacker from interacting with the hypervisor through another guest?A.   ContainersB.   VM escape protectionC.   Security brokerD.   Virtual desktopAnswer: BQUESTION 1344An internal intranet site is required to authenticate users and restrict access to content to only those who are authorized to view it. The site administrator previously encountered issues with credential spoofing when using the default NTLM setting and wants to move to a system that will be more resilient to replay attacks. Which of the following should the administrator implement?A.   NTLMv2B.   TACACS+C.   KerberosD.   ShibbolethAnswer: CQUESTION 1345A security consultant is analyzing data from a recent compromise. The following data points are documented:- Access to data on share drives and certain networked hosts was lost after an employee logged in to an interactive session as a privileged user.- The data was unreadable by any known commercial software.- The issue spread through the enterprise via SMB only when certain users accessed data.- Removal instructions were not available from any major antivirus vendor.Which of the following types of malware is this an example of?A.   RATB.   RansomwareC.   BackdoorD.   KeyloggerE.   WormAnswer: BQUESTION 1346An organization handling highly confidential information needs to update its systems. Which of the following is the BEST method to prevent data compromise?A.   WipingB.   DegaussingC.   ShreddingD.   PurgingAnswer: CQUESTION 1347A security administrator is working with the human resources department to classify data held by the company. The administrator has determined the data contains a variety of data types, including health information, employee names and addresses, trade secrets, and confidential customer information. Which of the following should the security administrator do NEXT?A.   Apply a predefined set of labels from government sources to all data within the companyB.   Create a custom set of data labels to group the data by sensitivity and protection requirementsC.   Label sensitive data according to age to comply with retention policiesD.   Destroy company information that is not labeled in compliance with government regulations and lawsAnswer: BQUESTION 1348A security administrator has been conducting an account permissions review that has identified several users who belong to functional groups and groups responsible for auditing the functional groups' actions. Several recent outages have not been able to be traced to any user. Which of the following should the security administrator recommend to preserve future audit log integrity?A.   Enforcing stricter onboarding workflow policiesB.   Applying least privilege to user group membershipC.   Following standard naming conventions for audit group usersD.   Restricting audit group membership to service accountsAnswer: CQUESTION 1349Joe, a new employee, discovered a thumb drive with the company's logo on it while walking in the parking lot. Joe was curious as to the contents of the drive and placed it into his work computer. Shortly after accessing the contents, he noticed the machine was running slower, started to reboot, and displayed new icons on the screen. Which of the following types of attacks occurred?A.   Social engineeringB.   Brute force attackC.   MITMD.   DoSAnswer: AQUESTION 1350In the event of a security incident, which of the following should be captured FIRST?A.   An external hard driveB.   System memoryC.   An internal hard driveD.   Network interface dataAnswer: BQUESTION 1351A security analyst receives the following output:

Time	Action	Host	File Name	User
...	... policy ... blocked ...	...	Fingers ...	User1

Which of the following MOST likely occurred to produce this output?A.   The host-based firewall prevented an attack from a Trojan horseB.   USB-OTG prevented a file from being uploaded to a mobile deviceC.   The host DLP prevented a file from being moved off a computerD.   The firewall prevented an incoming malware-infected fileAnswer: CQUESTION 1352Which of the following BEST explains "likelihood of occurrence"?A.   The chance that an event will happen regardless of how much damage it may causeB.   The overall impact to the organization once all factors have been consideredC.   The potential for a system to have a weakness or flaw that might be exploitedD.   The probability that a threat actor will target and attempt to exploit an organization's systemsAnswer: DQUESTION 1353When choosing a hashing algorithm for storing passwords in a web database, which of the following is the BEST explanation for choosing HMAC-MD5 over simple MD5?A.   HMAC provides hardware acceleration, thus speeding up authenticationB.   HMAC adds a transport layer handshake, which improves authenticationC.   HMAC-MD5 can be decrypted faster, speeding up performanceD.   HMAC-MD5 is more resistant to brute forcingAnswer: BQUESTION 1354Given the following:

```
> md5.exe file1.txt
> AD1FAB103773DC6A1E6021B7F503A210
> md5.exe file2.txt
> AD1FAB103773DC6A1E6021B7F503A210
```

Which of the following concepts of cryptography is shown?A.   CollisionB.   SaltingC.   SteganographyD.   Stream cipherAnswer: BQUESTION 1355A law firm wants to protect its customers' individual information, which is stored at a remote facility, from inadvertently being compromised through a violation of the security objectives. Which of the following BEST describes the customer information that is being stored at this facility?A.   Trade secretsB.   Personal health informationC.   ProprietaryD.   ConfidentialAnswer: DQUESTION 1356A technician wants to configure a wireless router at a small office that manages a family-owned dry cleaning business. The router will support five laptops, personal smartphones, a wireless printer, and occasional guests. Which of the following wireless configurations is BEST implemented in this scenario?A.   Single SSID with WPA2-EnterpriseB.   802.1X with a guest VLANC.   Dual SSID with WPA2-PSKD.   Captive portal with two-factor authenticationAnswer: CQUESTION 1357A systems administrator just issued the ssh-keygen ?t rsa command on a Linux terminal. Which of the following BEST describes what the rsa portion of the command represents?A.   A key generation algorithmB.   A hashing algorithmC.   A public key infrastructure typeD.   A certificate authority typeAnswer: AQUESTION 1358A newly hired Chief Security Officer (CSO) is reviewing the company's IRP and notices the procedures for zero-day malware attacks are being poorly executed, resulting in the CSIRT failing to address and coordinate malware removal from the system. Which of the following phases would BEST address these shortcomings?A.   IdentificationB.   Lessons learnedC.   RecoveryD.   PreparationE.   EradicationAnswer: BQUESTION 1359A security analyst has identified malware that is propagating automatically to multiple systems on the network. Which of the following types of malware is MOST likely impacting the network?A.   VirusB.   WormC.   Logic bombD.   BackdoorAnswer: BQUESTION 1360An organization allows the use of open-source software as long as users perform a file integrity check on the executables and verify the file against hashes of known malware. A user downloads the following files from an open-source website:

FILE NAME	MD5
webserver_81.exe	1e39 2210 faec 6ac4 243f 22cd 33da 62e4
opendatabase_43.exe	e39a 1140 bc90 232f 2010 6e28 d6e3
webserver_82.exe	2f40 3221 33ad 8f34 1032 1adc 13ef 51a4
opendatabase_44.exe	2a22 10ac 36ac 7789 10af 12aa 23aa 51e6

After submitting the hashes to the malware registry, the user is alerted that 2f40 3221 33ad 8f34 matches a known malware signature. The organization has been running all of 1032 1adc 13ef 51a4 the above software with no known issues. Which of the following actions should the user take and why?A.   Download and run the software but notify the organization's cybersecurity office. The malware registry has a false positive since the software has been running without any issues.B.   Do not run any of the software and notify the organization's cybersecurity office. The open-source website has been compromised, and none of the software can be trusted.C.   Download and run only webserver_82.exe and opendatabase_44.exe and notify the organization's cybersecurity office. Legacy versions of the software have been compromised.D.   Do not run webserver_82.exe and notify the organization's cybersecurity office. The software is malware.Answer: DQUESTION 1361An administrator needs to protect five websites with SSL certificates. Three of the websites have different domain names, and two of the websites share the domain name but have different subdomain prefixes. Which of the following SSL certificates should the administrator purchase to protect all the websites and be able to administer them easily at a later time?A.   One SAN certificateB.   One Unified Communications Certificate and one wildcard certificateC.   One wildcard certificate and two standard certificatesD.   Five standard certificatesAnswer: AQUESTION 1362A security administrator begins assessing a network with software that checks for available exploits against a known database, using both credentials and external scripts. A report will be compiled and used to confirm patching levels. This is an example of:A.   penetration testingB.   fuzzingC.   static code analysisD.   vulnerability scanningAnswer: DQUESTION 1363While testing a new application, a developer discovers that the inclusion of an apostrophe in a username causes the application to crash. Which of the following secure coding techniques would be MOST useful to avoid this problem?A.   Input validationB.   Code signingC.   ObfuscationD.   EncryptionAnswer: AQUESTION 1364A company recently contracted a penetration testing firm to conduct an assessment. During the assessment, the penetration testers were able to capture unencrypted communication between directory servers. The penetration testers recommended encrypting this communication to fix

the vulnerability. Which of the following protocols should the company implement to close this finding?A.   DNSSECB.   SFTPC.   KerberosD.   LDAPSAnswer: DQUESTION 1365Which of the following are disadvantages of full backups? (Choose three.)A.   They rely on other backups for recoveryB.   They require the most storageC.   They demand the most bandwidthD.   They have the slowest recovery timeE.   They are impossible in virtual environmentsF.   They require on-site storageG.   They are time-consuming to completeAnswer: BDGQUESTION 1366A security analyst performs a vulnerability scan on the local network. Several items are flagged on the report as being critical issues. The security analyst researches each of the vulnerabilities and discovers that one of the critical issues on the report was mitigated in a previous scan. Which of the following MOST likely happened?A.   A patch was removedB.   A false positive occurredC.   The tool has a high crossover error rateD.   A necessary service was not runningAnswer: BResources From:1.2021 Latest Braindump2go SY0-501 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/sy0-501.html2.2021 Latest Braindump2go SY0-501 PDF and SY0-501 VCE Dumps Free Share: https://drive.google.com/drive/folders/1Mto9aYkbmrvlHB5IFqCx-MuIqEVJQ9Yu?usp=sharing3.2021 Free Braindump2go SY0-501 Exam Questions Download:https://www.braindump2go.com/free-online-pdf/SY0-501-Dumps(1336-1366).pdf https://www.braindump2go.com/free-online-pdf/SY0-501-PDF-Dumps(1293-1314).pdf https://www.braindump2go.com/free-online-pdf/SY0-501-VCE-Dumps(1315-1335).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!