KTest

更に上のクオリティ　更に上のサービス

問題集

http://www.ktest.jp

1年で無料進級することに提供する

Exam : **HP0-276**

Title : OpenVMS Version 7.x to 8.2 Migrarion

Version : Demo

1. Click the Exhibit button. Which user is logged in via SSH?

```
$ show user /full
      OpenVMS user Processes at 30-JAN-2006
12:23:31.25
    Total number of users = 5,  number of
processes = 5

 username Process Name  PID       Terminal
 SYSTEM   SYSTEM        0000013E  OPA0:
 BOND     007           0000013A  TNA19:
(Host: 192.168.0.2 Port:1036)
 M        M             0000013F  RTA1:
(NET23::USER109)
 Q        Q             0000013D  FTA1:
 ?edited for brevity □
$
```

A. Q

B. BOND

C. SYSTEM

D. M

Answer: A

2. What is the maximum length of an OpenVMS username in the default configuration?

A. 12 characters

B. 16 characters

C. 20 characters

D. 24 characters

Answer: A

3. What is the purpose of "erase on delete"?

A. ensure that disk blocks are removed from the user's disk quota

B. ensure that disk blocks are written regularly to avoid subsequent bad block errors

C. overwrite file data to flush original disk blocks from XFC (eXtended File Cache) memory

D. overwrite file data in every block to prevent subsequent 'scavenging' of reallocated disk blocks

Answer: D

4. Which feature of OpenVMS allows verification of the integrity and authenticity of product installation kits?
A. sFTP

B. DCE Remote Procedure Call

C. Kerberos with Secure Delivery
D. PCSI with Secure Delivery based
on CDSA

Answer: D

5. A system manager wants to ensure that non-privileged users can only access those files for which they already know the file name. How can files in a directory be protected so this is accomplished?
A. set directory protection to execute, and file access as required
B. set directory protection to control, and file access as required
C. set directory protection to no access, and file access as required
D. it is not possible to
do this

Answer: A

6. User PHILBY, UIC [SIS,PHILBY], holds rights identifiers LONDON and CAMBRIDGE and executes the command TYPE *.* in a directory containing the following files. Which file will cause auditing messages to be sent to the security operator consoles?
A. SOVIET.DAT [SIS,MACLEAN] (RWED,RWED,RE,)
(ALARM=SECURITY,ACCESS=READ+FAILURE)
(IDENTIFIER=OXFORD,ACCESS=READ)
(IDENTIFIER=HARVARD,ACCESS=NONE)
B. AMERICAN.DAT
[CIA,BURGESS](RWED,RWED,,)
(IDENTIFIER=LONDON,ACCESS=NONE)
(IDENTIFIER=CAMBRIDGE,ACCESS=READ)
(AUDIT=SECURITY,ACCESS=READ+SUCCES
S)
C. BRITISH.DAT [CIA,BLUNT] (RWED,RWED,,)
(ALARM=SECURITY,ACCESS=READ+SUCCESS)
(IDENTIFIER=CAMBRIDGE,ACCESS=READ)
(IDENTIFIER=LONDON,ACCESS=NONE)
D. GERMAN.DAT [SYSTEM] (RWED,RWED,RE,)
(AUDIT=SECURITY,ACCESS=READ+FAILURE)

(IDENTIFIER=OXFORD,ACCESS=NONE)
(DEFAULT_PROTECTION,ACCESS=READ)

Answer: C

7. What are three OpenVMS protected object classes? Select three.
A. user
B. XFC cache
C. global section
D. event flag cluster
E. logical name table

Answer: CDE

8. What are five valid characters in OpenVMS passwords within the default configuration? Select five.
A. letters A-Z (case insensitive)
B. multinational (accented) letters
C. digits 0-9
D. dot (.)
E. space ( )
F. dollar $
G. underscore (_)

Answer: ACEFG

9. What are two elements of CLUSTER_AUTHORIZE.DAT? Select two.
A. cluster number
B. cluster incarnation time
C. cluster password
D. cluster account passwords
E. cluster authorized interconnects

Answer: AC

10. What is the purpose of "high water marking"?
A. limit the use of XFC (eXtended File Cache) buffers
B. prevent a process from exhausting its FILLM quota C. prevent an application from writing file data beyond the disk quota limit

D. prevent reading file data beyond the point in a file which has been written

Answer: D

11. Which three are valid components of an object's security profile? Select three.
A. object owner
B. access control list
C. process quotas
D. alarm journal entry
E. object protection mask
Answer: ABE

12. Which two objects are accessible to processes with specific authorized privileges enabled? Select two.
A. queues are read/write accessible to processes with OPER privilege
B. VMSMAIL and Internet mail are read/write accessible to users with NETMBX privilege
C. the user authorization file is read/write accessible to processes with WORLD privilege
D. system logical name tables are read/write accessible to processes with SYSNAM privilege
E. page and swap file contents are read/write accessible to processes with PSWAPM privilege Answer: AD

13. Which two options are valid access modes (e.g. in AUTHORIZE)? Select two.
A. BATCH
B. DETACHED
C. NETWORK
D. PRIVILEGED
E. SUPERVISOR
Answer: AC

14. What is the default protection mask set by the system parameter RMS_FILEPROT value=64000 (decimal)?
A. (S:RWED,O:RWED,G:RE,W:)
B. (S:RWE,O:RWE,G:RE,W:RE)
C. (S:RWED,O:RWED,G:RE,W:RE) D. (S:RWE,O:RWE,G:RE,W:RE)

Answer: A

15. When writing secure command procedures, why should READ/PROMPT be used instead of INQUIRE?
A. because INQUIRE only works with captive accounts
B. because INQUIRE echoes user input back to the terminal by default
C. because READ/PROMPT does not perform symbol substitution on the user input
D. because READ/PROMPT creates an audit trail record in SECURITY.AUDIT$JOURNAL

Answer: C

16. A backup system disk copy is missing. What are two of the vulnerabilities that are introduced? Select two.
A. protected system files and data can be read
B. licenses can be extracted from LMF$LURT.DAT
C. usernames and their associated privileges can be listed
D. passwords can be directly extracted from SYSUAF.DAT
E. passwords can be directly extracted from

VMS$PASSWORD_HISTORY.DATA

Answer: AC

17. Policy requires that a particularly sensitive application is available only when two specific users are present. What is the relevant OpenVMS security mechanism?
A. an application-specific captive account with primary and secondary passwords
B. two non-privileged accounts with synchronized passwords
C. two-factor authentication
D. ACL access to the application

Answer: A

18. Which two mechanisms allow authentication of network access to a system without explicit login? Select two.
A. SSH
B. LDAP
C. proxy account
D. active directory
E. Advanced Server

Answer: AC

19. An organization has several OpenVMS clusters. How can you ensure a single sign-on authentication mechanism with a common password across all clusters?
A. this is not possible
B. copy the SYSUAF file from a master cluster to the other clusters once a day
C. the same password on multiple clusters is permitted when clusters have a "trust" relationship between accounts (eg: proxy accounts)
D. implement an external authentication
mechanism Answer: D

20. What two benefits can account quotas provide on an OpenVMS system? Select two.
A. user and group (departmental) chargeback capabilities
B. allows interactive users to run faster than batch jobs
C. allow different behaviors for multiple applications at the same time
D. minimize the impact of users or applications on other users
E. maximize throughput of specially-designed applications on
OpenVMS systems

Answer: CD

21. Which two security threats are generally unsuccessful on an OpenVMS system? Select two.
A. buffer overflow attacks
B. virus attacks
C. unsecured network
D. disgruntled employees
E.socialengin
eering
Answer: AB

22. Which passwords can potentially be determined with a LAN packet capture tool? Select two.
A. SYSTEM password
B. default DECnet account password
C. user account passwords
D. TCP/IP Services SSH password E. cluster authorization password

Answer: AC

23. OpenVMS systems are highly resistant to buffer overflow attacks. What is one reason for this?

A. system services first ensure that the calling application has write access to the entire specified buffer space
B. consequent usage of NULL-terminated strings precludes buffer overflow attacks
C. only users holding the VMS$BUFFER_OBJECT_USER rights identifier are allowed to use buffers
D. buffer cannot grow beyond the minimum of WSDEF and MAXBUF, precluding buffer overflow attacks

Answer: A

24. Which mechanism can be used to prevent unauthorized access to the hardware console settings?
A. disable hardware reboot parameter block
B. console password
C. OpenVMS privileges
D. set console boot_secure flag
E. auto-boot on power-up or system crash

Answer: B

25. When an account is no longer in use, what actions prevent the account from being used while still permitting subsequent backup and restoration of data with original security attributes such as ownership?
A. immediately remove the files and retain the account
B. immediately remove the account and ensure files have been backed up
C. no immediate action, routine "unused account" review will suffice
D. immediately DISUSER the account and ensure files have been backed up

Answer: D

26. Why does an OpenVMS system with both internal and external users need to be protected by a hardware firewall?
A. to prevent usage of the OpenVMS system as a spam relay
B. the firewall caches requests when the OpenVMS system is overloaded
C. the firewall translates between big and little endian data in the network packets
D. to protect the OpenVMS system against network threats such as a DoS attack
Answer: D

27. What can be done to prevent IP node spoofing within an OpenVMS environment?

A. physically secure the network

B. implement reverse ARP passwords

C. enable secure DNS
D.enforceauthenticated
SMTP

Answer: A

28. Which OpenVMS command is used to show active TCP connections?
A. TCPIP> netstat -n
B. TCPIP> show known link
C. NCL> show session control port * all
D. LANCP> show device/connection
E. TCPIP>show
portmapper

Answer: A

29. When setting up the disk and file structures for user data, which techniques are used to control access? Select TWO.
A. disk quotas
B. protection masks
C. highwater marking
D. Access Control Lists
E. rooted logical
names

Answer: BD

30. Given a separate copy of an OpenVMS UAF, which statement is true regarding attempts to retrieve a given user's password? Select two.
A. Password guesses can be tested using a "brute force" method.
B. Attempts to attack the file by "brute force" will result in the file triggering security alarms.
C. Passwords are encrypted with a one way hash algorithm, so password retrieval is not feasible.
D. Attempts will be unsuccessful without a cross reference to the
password history file.

Answer: AC