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

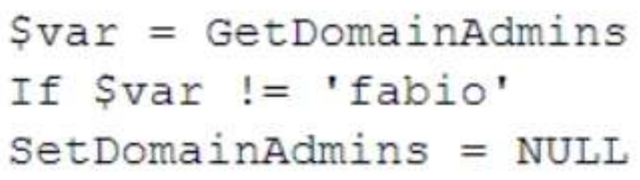
Visit Braindump2go and Download Full Version SY0-501 Exam Dumps

QUESTION 931
A security administrator is investigating a report that a user is receiving suspicious emails. The user's machine has an old functioning modem installed. Which of the following security concerns need to be identified and mitigated? (Select TWO).

A. Vishing
B. Whaling
C. Spear phishing
D. Pharming
E. War dialing
F. Hoaxing

Answer: EF

QUESTION 932
A security administrator found the following piece of code referenced on a domain controller's task scheduler:



```
$var = GetDomainAdmins
If $var != 'fabio'
SetDomainAdmins = NULL
```

With which of the following types of malware is the code associated?

A. RAT
B. Backdoor
C. Logic bomb
D. Crypto-malware

Answer: C

QUESTION 933
A forensic investigation discovered that accounts belonging to employees who were terminated numerous years ago were recently used to gain unauthorized access on a company's web servers. Which of the following controls would reduce the risk of this reoccurring? (Select TWO)

A. Enable time-of-day restrictions.
B. Disable inactive accounts on a timely basis.

C. Increase the password complexity requirements.
D. Run regular account usage audits.
E. Set expiration dates for all temporary accounts.
F. Prohibit the use of shared accounts in an AUP.

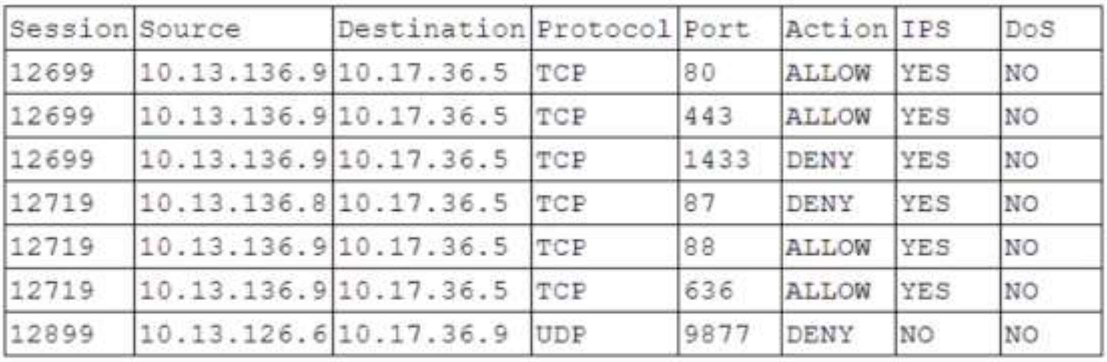
Answer: BE

QUESTION 934
Which of the following is the MOST significant difference between intrusive a non-intrusive vulnerability scanning?

A. One uses credentials, but the other does not
B. One has a higher potential for disrupting system operations
C. One allows systems to activate firewall countermeasures.
D. One returns service banners, including running versions.

Answer: B

QUESTION 935
The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team's application is 10.13.136.9, and the destination IP is 10.17.36.5. The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:



Session	Source	Destination	Protocol	Port	Action	IPS	DoS
12699	10.13.136.9	10.17.36.5	TCP	80	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	443	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	1433	DENY	YES	NO
12719	10.13.136.8	10.17.36.5	TCP	87	DENY	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	88	ALLOW	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	636	ALLOW	YES	NO
12899	10.13.126.6	10.17.36.9	UDP	9877	DENY	NO	NO

Which of the following should the security analyst request NEXT based on the UTM firewall analysis?

A. Request the application team to allow TCP port 87 to listen on 10.17.36.5.
B. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5.
C. Request the network team to turn off IPS for 10.13.136.8 going to 10.17.36.5.
D. Request the application team to reconfigure the application and allow RPC Communication

Answer: A

QUESTION 936
A user is unable to obtain an IP address from the corporate DHCP server. Which of the following is MOST likely the cause?

A. Default configuration
B. Resource exhaustion
C. Memory overflow
D. Improper input handling

Answer: A

QUESTION 937

An authorized user is conducting a penetration scan of a system, for an organization. The tester has a set of network diagrams, source code, version numbers of applications, and other information about the system, including hostnames and network addresses. Which of the following BEST describes this type of penetration test?

A. Gray-box testing
B. Black-box testing
C. White-box testing
D. Blue team exercise
E. Red team exercise

Answer: C

QUESTION 938
Users in an organization access the network, systems, and all resources through multifactor, PIV-enabled SSO. Those logins are monitored and audited for unusual activity. This organization has a reputation for practicing good security hygiene disabling default and guest accounts. and enforcing temporary privilege escalation when administrative functions are necessary.
A recent security audit has uncovered suspicious privileged activity that cannot be attributed to any user. Which of the following is the BEST place to start investigating the source of the activity?

A. Use of privileged service accounts by individuals who know the passwords
B. Hidden guest accounts with default privileged access that can be accessed by outsiders
C. Default systems accounts that have not been disabled and are being used by insiders
D. Backdoor accounts that are part of the vendor-provided system installation

Answer: B

QUESTION 939
A forensic analyst is creating a report of findings for litigation purposes. The analyst must ensure data is preserved using all elements of the CIA triad. Given this scenario, which of the following should the analyst use to BEST meet these requirements?

A. Hashing for confidentiality, full backups for integrity, and encryption for availability
B. Full backups for confidentiality, encryption for integrity, and hashing for availability
C. Hashing for confidentiality, encryption for integrity, and full backups for availability
D. Encryption for confidentiality, hashing for integrity, and full backups for availability

Answer: D

QUESTION 940
A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Select TWO).

A. Use a unique managed service account.
B. Utilize a generic password for authenticating.
C. Enable and review account audit logs.
D. Enforce least possible privileges for the account.
E. Add the account to the local administrator's group.
F. Use a guest account placed in a non-privileged users' group.

Answer: DE

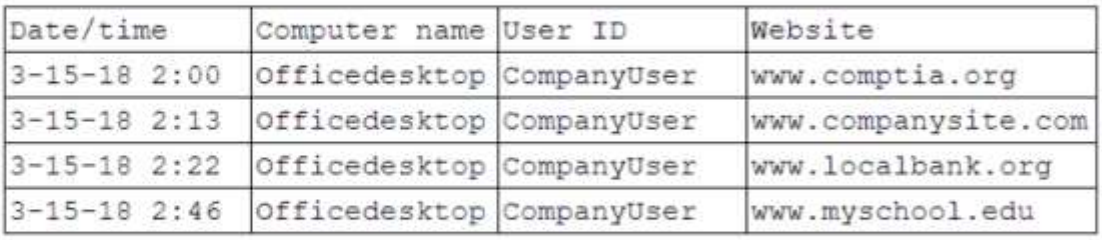
QUESTION 941

Which of the following is the MAIN disadvantage of using SSO?

A. The architecture can introduce a single point of failure.
B. Users need to authenticate for each resource they access.
C. It requires an organization to configure federation.
D. The authentication is transparent to the user.

Answer: A

QUESTION 942
Given the output. Which of the following account management practices should the security engineer use to mitigate the identified risk?



Date/time	Computer name	User ID	Website
3-15-18 2:00	Officedesktop	CompanyUser	www.comptia.org
3-15-18 2:13	Officedesktop	CompanyUser	www.companysite.com
3-15-18 2:22	Officedesktop	CompanyUser	www.localbank.org
3-15-18 2:46	Officedesktop	CompanyUser	www.myschool.edu

A. Implement least privilege.
B. Eliminate shared accounts.
C. Eliminate password reuse.
D. Implement two-factor authentication.

Answer: B