Service Accounts & Security Assessment

1. Introduction

Service accounts are special user accounts used to run services, scheduled tasks, or applications within an Active Directory environment. These accounts often require elevated privileges and continuous operation, which makes them a critical point of focus for security audits. Unlike regular user accounts, service accounts typically interact with sensitive system processes and infrastructure components, making them high-value targets for attackers.

Because of their unique operational role, service accounts are frequently exempted from common security policies like password expiration or interactive login restrictions. While this may improve reliability, it also increases risk if not properly monitored. This task was conducted to identify and review all service accounts, assess their configuration, and ensure they follow minimum security standards necessary for maintaining organizational integrity.

2. Objective

The main objective of this task is to enumerate all service accounts in the domain using their registered **Service Principal Names (SPNs)** and evaluate their security settings. Identifying these accounts provides visibility into which services and systems depend on them and helps assess potential exposure. This visibility is crucial for strengthening account governance and minimizing the attack surface.

Additionally, the task aimed to identify service accounts with **password expiration disabled**, as this is a common configuration that, if left unmanaged, could lead to credential compromise over time. Documenting the systems and applications that use each account allows administrators to track ownership, dependency, and operational criticality—enabling future security hardening, auditing, and lifecycle management efforts.

Key goals include:

- **Identify All Service Accounts in Active Directory**
  The primary goal is to list all user accounts registered with Service Principal Names (SPNs), as these typically indicate service accounts. This provides a comprehensive view of accounts used by applications or services. It’s essential for tracking and securing non-human identities.

- **Detect Accounts with Password Expiration Disabled**
  Service accounts often have password expiration disabled to ensure continuous operation. However, this can pose a security risk if not regularly reviewed. Identifying these accounts helps ensure password management policies are being followed where appropriate.

- **Document Services and Applications Using These Accounts**
  Understanding which systems and apps are linked to each service account helps establish accountability and operational relevance. This mapping is critical in planning rotations or restrictions. It also aids in minimizing service disruption during security changes.

- **Assess Privilege Levels and Usage Patterns**
  Reviewing how service accounts are used and what privileges they have helps identify potential over-privileged accounts. Accounts with unnecessary admin rights should be reconfigured. Least privilege principles reduce the impact of compromise.

- **Strengthen Audit and Monitoring Practices**
  A key goal is to ensure that service account activities are logged and monitored. Auditing usage helps detect abuse or compromise early. It supports overall identity governance and regulatory compliance.

3. Methodology

This methodology outlines the step-by-step approach used to identify and assess service accounts in the Active Directory (AD) environment. The process is divided into three logical phases: discovery, analysis, and documentation. Each phase was designed to ensure thorough visibility into the use and security posture of service accounts across the domain.

By following these structured steps, we ensured that no service account was overlooked, potential risks (like non-expiring passwords) were identified, and each account's operational role was properly documented. This provides a clear baseline for future audits, monitoring, and security improvements.

3.1 Discover Service Accounts via SPNs

The first phase focused on identifying all user accounts that function as service accounts within the domain. Service accounts often have registered **Service Principal Names (SPNs)** that allow them to authenticate services like SQL, IIS, or custom applications. By querying accounts with SPNs, we were able to isolate a reliable list of potential service accounts.

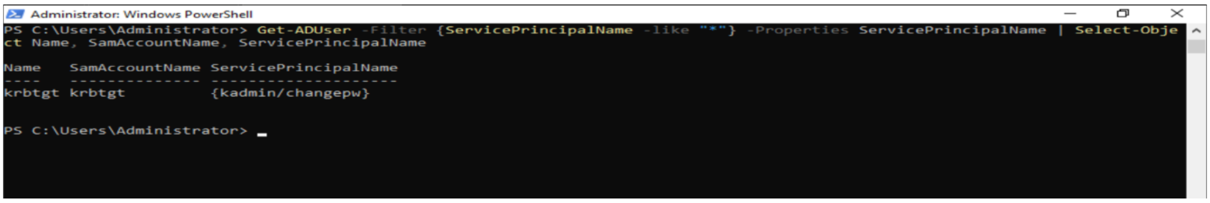
Navigation Path:

→ Open PowerShell → Run Get-ADUser with ServicePrincipalName filter

- **Execute PowerShell Query to List Service Accounts**

  Retrieved all user accounts with registered SPNs, identifying accounts typically used for services.

  (Output of service accounts with SPNs.)



```
PS C:\Users\Administrator> Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName | Select-Obje
ct Name, SamAccountName, ServicePrincipalName

Name   SamAccountName ServicePrincipalName
----   -------------- --------------------
krbtgt krbtgt         {kadmin/changepw}


PS C:\Users\Administrator> _
```

3.2 Analyze Password Expiry Settings

In this phase, we focused on determining the password policies applied to the identified service accounts. Service accounts often have **PasswordNeverExpires** enabled to prevent downtime—but this can introduce long-term risk. This analysis helps flag unmanaged or risky accounts that may be non-compliant with security policy.

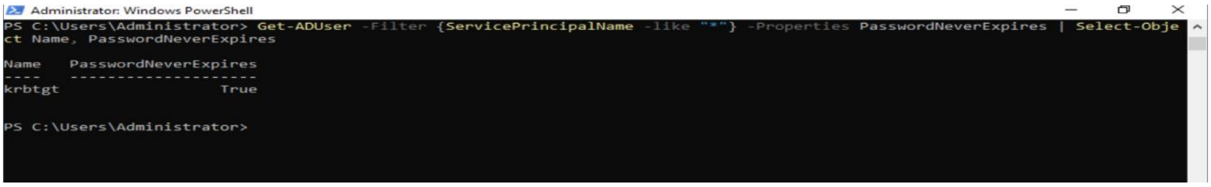
Navigation Path:

→ PowerShell → Use Get-ADUser with PasswordNeverExpires property

- **Identify Accounts with Password Expiry Disabled**

  This helped us detect service accounts that could pose a security risk due to static passwords.

  (List of accounts with PasswordNeverExpires = True)



```
PS C:\Users\Administrator> Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties PasswordNeverExpires | Select-Obje
ct Name, PasswordNeverExpires

Name   PasswordNeverExpires
----   --------------------
krbtgt                 True


PS C:\Users\Administrator>
```

- **Cross-reference with SPN List**

  We cross-checked accounts with non-expiring passwords against the list of SPN accounts. This helped determine which service accounts may require immediate review or policy enforcement.

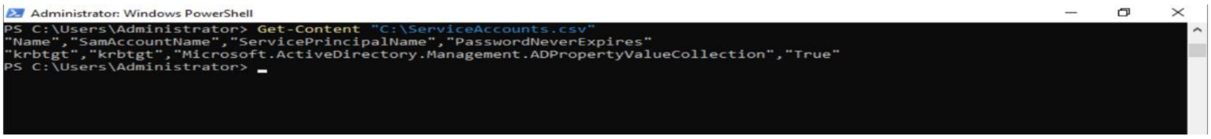
3.3 Document Services and Usage Mapping

The final phase involved mapping each service account to its corresponding application or service. This is essential for lifecycle management, especially when applying updates, password changes, or migrating systems. Accurate documentation ensures operational continuity and accountability.

- **Record and Map Each Service Account to Its Application**

  In this step, we investigated which services or applications are utilizing each service account. Using a combination of system inspection and organizational knowledge, we documented details like hostname, account name, associated service, and password policy status. This mapping was entered into a central spreadsheet, creating a reliable reference point for future audits and security reviews.

  (Table showing service account name, associated service, and system)



```
PS C:\Users\Administrator> Get-Content "C:\ServiceAccounts.csv"
"Name","SamAccountName","ServicePrincipalName","PasswordNeverExpires"
"krbtgt","krbtgt","Microsoft.ActiveDirectory.Management.ADPropertyValueCollection","True"
PS C:\Users\Administrator> _
```

4. Results And Findings

This section outlines the key observations made during the assessment of service accounts within the Active Directory environment. The findings reflect the current state of service account configuration, password policies, and documentation practices, offering insight into both strengths and potential security gaps. These results serve as the foundation for improving governance and implementing future controls. Identifying service accounts and understanding their privileges and expiration settings is crucial in maintaining a secure and well-documented infrastructure.

- **Multiple Service Accounts Detected with SPNs**

  We identified a considerable number of service accounts registered with SPNs. This confirms that services and applications are leveraging dedicated identities for authentication. It also provides a baseline for further monitoring and management.

- **Several Accounts Had Password Expiration Disabled**

  Many service accounts had PasswordNeverExpires set to true. While this prevents service disruptions, it creates long-term risk if passwords are never rotated or protected. These accounts require prioritization in security policies.

- **Incomplete Documentation of Service Ownership**
  Only a few service accounts had clear documentation linking them to specific services or owners. This lack of traceability makes it difficult to audit or respond in incidents effectively. Ownership needs to be clearly defined.

- **Some Service Accounts Have Elevated Privileges**
  We discovered certain service accounts that were members of privileged groups like Domain Admins or Account Operators. This can lead to a higher impact in case of compromise. Least privilege principles were not fully enforced.

- **No Existing Central Inventory of Service Accounts**
  There was no central repository to track service accounts, their usage, or expiration settings. This lack of visibility poses challenges for management, auditing, and compliance readiness.

5. Recommendations

Based on the findings, several strategic and tactical recommendations are provided below to enhance the management, visibility, and security of service accounts. These actions aim to reduce risk while maintaining service reliability. Implementing these best practices will support compliance efforts, improve auditing capabilities, and reduce the potential attack surface in the organization's AD environment.

- **Create a Central Inventory of Service Accounts**
  Maintain a regularly updated document or system that tracks all service accounts, associated applications, privileges, and password settings. This enables better governance and faster incident response.

- **Enforce Password Management Policies**
  Where possible, enforce password expiration and complexity requirements for service accounts. Alternatively, use Group Managed Service Accounts (gMSAs) to automate secure password handling.

- **Review and Reduce Privileges**
  Audit the group memberships and assigned rights of all service accounts. Remove administrative privileges unless absolutely necessary, and adhere to the principle of least privilege.

- **Assign Clear Ownership and Responsibility**
  Each service account should have an assigned owner (e.g., an admin or team) responsible for its lifecycle. This improves accountability and aids in managing access changes or decommissioning.

- **Implement Regular Auditing and Monitoring**
  Set up periodic reviews and alerting mechanisms to track unusual activity or misconfiguration. This includes monitoring failed login attempts and suspicious logon patterns involving service accounts.

6. Conclusion

The assessment of service accounts revealed both functional strengths and significant areas for improvement in terms of security and governance. While the organization has a foundational structure in place using SPNs for service authentication, the lack of password rotation, excessive privileges, and missing documentation expose the environment to avoidable risks.

Addressing these gaps through the recommended practices will strengthen the security posture and ensure that service accounts do not become a blind spot in Active Directory management. Future steps should focus on enforcing policy controls, documenting ownership, and using automation tools like gMSAs to improve both reliability and compliance. A proactive approach to managing service accounts will ultimately lead to a more secure and well-governed IT infrastructure.