Security Report

Password Reuse Vulnerability Report

Summary

Found 3 instances of password reuse with administrative accounts.

Password reuse across administrative accounts significantly increases the risk of lateral movement and privilege escalation in the event of a single account compromise. If an attacker gains access to one system or user, reused credentials can enable access to other critical systems without further exploitation. This undermines segmentation and containment strategies, and may lead to full domain compromise, data breaches, and disruption of business operations.

Password Reuse Details

Admin Account	Reuse Accounts	Password
petrov.d.a_adm	sync_monitor api_stage report_test	1U***e2
popov.s.b_adm	monitor_qa report_live report_02 sync_01 backup_02	Us***23
Administrator	andreev.e.c orlov.u.c petrov.c.c popov.s.b	Not cracked

Admin Account	Reuse Accounts	Password
	andreev.j.m sidorov.a.y makarov.o.z andreev.c.r sokolov.e.b sidorov.v.f nikitin.g.g morozov.c.t popov.g.f soloviev.s.u sidorov.q.r egorov.v.w petrov.k.k	

Recommended Actions

- Use a tool for password analysis in Active Directory to identify reused passwords among domain accounts (e.g., AD Sonar — adsonar.ru).
- Define and enforce a policy that requires the use of unique, strong passwords for all administrative accounts to prevent reuse across systems and services.
- Implement automatic generation and scheduled rotation of unique, strong local administrator passwords for each computer using Microsoft LAPS (Local Administrator Password Solution).

Weak Passwords Vulnerability Report

Summary

Found 27 users with weak passwords, including 2 privileged and enabled accounts. As a result, passwords were recovered for 5.31% of users.

Weak passwords significantly increase the risk of unauthorized access to critical systems and sensitive data. If an attacker successfully compromises an account — especially one with elevated privileges — this can lead to full domain compromise, lateral movement across the network, data breaches, and disruption of business operations. The presence of active domain accounts with weak or compromised passwords presents a critical vulnerability in the organization's security posture.

Users with Weak Passwords

Username	Password	Domain Admin	Status
petrov.d.a_adm	1U***e2	Yes	Active
popov.s.b_adm	Us***23	Yes	Active
monitor_qa	Us***23	No	Active
fedorov.m.z	Se***y1	No	Active
soloviev.a.y	Pa***1!	No	Active
romanov.z.m	Pa***1!	No	Active
kotkov.r.n	Pa***1!	No	Active
kotkov.x.t	Pa***1!	No	Active
nikolaev.x.k	Se***y1	No	Active
stepanov.j.d	Pa***1!	No	Active
karpov.o.b	Pa***1!	No	Active
egorov.l.p	Pa***1!	No	Active
grigoriev.b.g	Pa***1!	No	Active
kotkov.w.s	Pa***1!	No	Active
popov.e.f	Pa***1!	No	Active
mikhailov.q.n	Se***y1	No	Active
yakovlev.v.p	Se***y1	No	Active
smirnov.i.m	Pa***1!	No	Active
mikhailov.o.l	Pa***1!	No	Active
kuznetsov.u.b	Pa***1!	No	Active
report_live	Us***23	No	Active
sync_monitor	1U***e2	No	Active
report_02	Us***23	No	Active
api_stage	1U***e2	No	Active

Username	Password	Domain Admin	Status
sync_01	Us***23	No	Active
report_test	1U***e2	No	Active
backup_02	Us***23	No	Active

Recommended Actions

- Use a tool for password analysis in Active Directory to identify weak, common, or compromised passwords among domain accounts (e.g., AD Sonar — adsonar.ru).
- Define and enforce a password policy that requires a minimum password length of 12 characters, including numbers, uppercase and lowercase letters, and special characters. Domain accounts should be locked indefinitely after 5 failed login attempts, with manual unlocking required. This policy should be implemented through Group Policy Objects (GPO) or equivalent mechanisms.
- Avoid using common (dictionary-based) or easily guessable passwords. When developing a password policy, include examples of known weak password types.
- Use monitoring tools to detect online password brute-force attacks.

Reversible Encryption Vulnerability Report

Summary

Found 3 accounts with reversible encryption enabled.

When reversible encryption is enabled for an account in Active Directory, the password is stored in a format that can be easily decrypted to plain text by any process or user with the appropriate permissions. This significantly increases the risk of credential exposure through misconfigured access rights, backups, or compromised systems. If such an account has administrative privileges or is used in service integrations, an attacker gaining access to the decrypted password may escalate privileges or move laterally within

the domain. Reversible encryption should only be used in rare, justified scenarios, as it weakens the overall security posture of the environment.

Vulnerable Accounts Details

Account	Type	Status	Admin Rights	Password
kotkov.q.i	USER	Enabled	No	J@***13
kuznetsov.h.h	USER	Enabled	No	PA***OS
yakovlev.x.a	USER	Enabled	No	pr***al

Recommended Actions

- Disable reversible password encryption for all user accounts, unless explicitly required for a specific application or authentication mechanism.
- Review domain and local password policies to ensure that reversible encryption is not enabled by default.
- Educate administrators on the risks of reversible encryption and establish guidelines for secure password storage practices.
- Monitor Group Policy Objects (GPO) and account creation processes to prevent unintended re-enablement of reversible encryption settings.

Passwords in Description Vulnerability Report

Summary

Found 3 accounts with passwords in their descriptions.

Storing passwords in the description field of Active Directory accounts exposes sensitive credentials in clear text to any user or process with read access to directory attributes. This significantly increases the risk of credential theft, especially if the affected accounts have

administrative privileges or are active. An attacker with basic read access to the domain could easily harvest these passwords, potentially leading to unauthorized access, privilege escalation, and full domain compromise.

Vulnerable Accounts Details

Account	Status	Admin Rights	Password	Description
pavlov.s.s	Enabled	No	h* * *8*a*|*Password* : *h*%Lv5KaGfJqY8a	
romanov.m.a	Enabled	No	$w***9(	Password: $wG1shBX^ovM
sync_test	Enabled	No	FN***4!	Password: FNWRle0kSai5B

Recommended Actions

- Remove any plaintext passwords or other sensitive data from the description fields of all accounts.
- Review account descriptions across the domain to ensure they do not contain confidential or security-relevant information.
- Educate administrators and support staff on the risks of storing passwords or sensitive data in non-secure fields such as account descriptions.
- Implement role-based access controls (RBAC) to restrict read access to account attributes where possible.

Kerberoasting Vulnerability Report

Summary

Found 6 service accounts with cracked SPN passwords, including 1 privileged and enabled accounts. Kerberoasting attacks target service accounts with registered SPNs by requesting their Kerberos service tickets and attempting to crack them offline. If successful, the attacker obtains the clear-text password of the associated service account. These accounts often have elevated privileges or broad access within the domain. As a result, Kerberoasting can lead to privilege escalation, unauthorized access to critical systems, and facilitate further lateral movement across the network, potentially compromising the entire domain.

Vulnerable Service Accounts

Username	SPN	Password	Domain Admin
popov.s.b_adm	http/dc.vulnad.local	Us***23	Yes
vasiliev.s.i	IMAP/ SQL01.local.vulnad.local:21800 HTTP/ WEB02.corp.vulnad.local:42031 MSSQLSvc/ SQL02.corp.vulnad.local:38031	***	No
pavlov.i.k	IMAP/WEB01.corp.vulnad.local HTTP/ SQL02.internal.vulnad.local:65187	***	No
sidorov.i.e	HOST/EXCH02.corp.vulnad.local CIFS/ EXCH01.corp.vulnad.local:65478 MSSQLSvc/ SQL02.local.vulnad.local:26685	***	No
mikhailov.q.n	CIFS/SQL01 HOST/ WEB02.corp.vulnad.local:46048	Se***y1	No
yakovlev.v.p		Se***y1	No

Username	SPN	Password	Domain Admin
	HOST/ SQL01.local.vulnad.local:55683 HTTP/ WEB01.local.vulnad.local:16209 CIFS/DC01		

Recommended Actions

- Use a tool for password analysis in Active Directory to identify weak or easily crackable passwords among accounts with registered SPNs (e.g., AD Sonar — adsonar.ru).
- Use only non-privileged accounts to run services whenever possible. Service accounts should have the minimum necessary permissions required to function.
- Replace traditional service accounts with Group Managed Service Accounts (gMSA), which provide automatic password management and eliminate the need for manually set, potentially weak or reused passwords (Learn more about gMSA).
- Regularly audit Active Directory for accounts with SPNs and identify those with elevated privileges. Eliminate unnecessary privileges or unused SPNs.
- Implement strict password policies for all accounts with SPNs, ensuring strong, complex, and regularly rotated passwords.
- Monitor for abnormal Kerberos ticket requests and service ticket activity to detect signs of Kerberoasting attempts.

Pre-Windows 2000 Compatibility Vulnerability Report

Summary

Found 7 users with Pre-2000 compatibility enabled.

When a computer account is pre-created in Active Directory with the “Pre-Windows 2000” compatibility option enabled, it is assigned a predictable default password based on the computer name (typically the lowercase name without the trailing ‘$’). An attacker who knows or can guess the computer name may authenticate using this weak password. This can lead to unauthorized domain access, potential privilege escalation, and lateral movement within the network. Such accounts are often overlooked during password audits, increasing the long-term risk of compromise.

Vulnerable Computers

Computer	Password	Status
EXCH01$	EXCH01	Enable
APP02$	APP02	Enable
FILE01$	FILE01	Enable
DC02$	DC02	Enable
FILE02$	FILE02	Enable
SRV01$	SRV01	Enable
SQL02$	SQL02	Enable

Recommended Actions

- Regularly audit computer accounts in Active Directory and remove those that are unused or were created for legacy systems.
- Use tools such as Pre2k or NetExec (nxc) to identify computer accounts with the UserAccountControl value of 4128 (PASSWD_NOTREQD | WORKSTATION_TRUST_ACCOUNT), which indicates pre-created accounts with predictable default passwords.
- For identified accounts, set unique and strong passwords that are resistant to brute-force attacks.
- When creating new computer accounts, avoid using the “Assign this computer account as a pre-Windows 2000 computer” option to prevent assigning predictable passwords based on the computer name.

AS-REP Roasting Vulnerability Report

Summary

Found 5 accounts vulnerable to AS-REP Roasting, including 4 privileged and enabled accounts. AS-REP Roasting targets user accounts that do not require Kerberos pre-authentication. An attacker can request authentication data (AS-REP) for such accounts without knowing their password and then perform offline brute-force or dictionary attacks to recover the clear-text password. If successful, this may lead to unauthorized access, privilege escalation, and further lateral movement within the network. The risk is especially critical if affected accounts have elevated privileges or are used for service operations.

Vulnerable Users

Username	Password	Status
semenov.h.n	Not cracked	Enable
fedorov.m.z	Se***y1	Enable
nikolaev.x.k	Se***y1	Enable
mikhailov.r.o	Not cracked	Enable
mikhailov.a.g	Not cracked	Disable

Recommended Actions

- Use a tool for password and account configuration analysis in Active Directory to identify accounts vulnerable to AS-REP Roasting — i.e., those with the “Do not require Kerberos preauthentication” flag enabled (e.g., AD Sonar — adsonar.ru).
- Disable the “Do not require Kerberos preauthentication” option (`DONT_REQUIRE_PREAUTH` flag) for all domain accounts, unless explicitly required for operational purposes. Special attention should be paid to accounts with elevated privileges.

- Where the use of this flag is operationally justified, apply compensating controls such as strong, non-dictionary passwords and close monitoring for abnormal Kerberos authentication requests.

Unconstrained Delegation Vulnerability Report

Summary

Found 2 accounts with unconstrained delegation enabled.

Unconstrained delegation allows a system or service to impersonate users and access other services on their behalf without restriction. When enabled, the credentials (including Kerberos Ticket Granting Tickets, or TGTs) of any user who authenticates to the delegated system can be cached and reused. If an attacker compromises such a system, they can extract TGTs from memory and impersonate privileged users — including domain admins — across the domain. This exposes the environment to high-risk attacks such as Golden Ticket forging and full domain compromise.

Vulnerable Accounts Details

Account	Type	Status
DC$	COMPUTER	Enabled
sokolov.u.i	USER	Enabled

Recommended Actions

- Identify and review all accounts and computers with unconstrained delegation enabled, especially those with elevated privileges or exposed to user authentication (e.g., domain-joined servers).
- Disable unconstrained delegation on all accounts and systems unless strictly required for legacy application compatibility.

- Where delegation is needed, use **constrained delegation** (`"Trust this user for delegation to specified services only"`) or **resource-based constrained delegation (RBCD)** as more secure alternatives.
- Isolate systems that require delegation into separate, hardened network segments and monitor them closely for unusual authentication behavior.
- Regularly audit delegation settings via scripts or tools to prevent reintroduction of insecure configurations.