INCIDENT RESPONSE REPORT

Kerberoasting & Identity Compromise Simulation

Incident ID: IR-2025-KRB-001

Date: 19 Nov 2025

Severity: High

Status: Resolved

Prepared By: Marius-Alexandru Datcu
Security Operations Analyst

Azure Active Directory Lab Environment

1. Executive Summary

1.1 Incident Overview

On 19 Nov 2025, the Security Operations Center (SOC) detected anomalous authentication activity within the Azure Active Directory environment. Real-time monitoring identified a "Kerberoasting" attack pattern targeting a critical service account (sql-service). The attacker attempted to extract service ticket hashes for offline cracking.

1.2 Impact Analysis

- **Affected Assets:** Domain Controller (VM-DC), Service Account (sql-service), Standard User Account (bob.john).
- **Data Loss:** None confirmed; however, the service account credential was considered compromised.
- **Operational Impact:** Minimal. The incident was contained before lateral movement could extend to the SQL databases.

1.3 Response & Resolution

The incident was identified in real-time via Microsoft Sentinel using custom behavioral analytics rules. The response team immediately contained the compromised user account used for initial access and reset the credentials for the targeted service account. Furthermore, hardening measures (specifically AES enforcement) were implemented to prevent recurrence.

2. Technical Analysis

2.1 Detection Vector

The incident was triggered by a custom detection rule in Microsoft Sentinel monitoring for specific Kerberos anomalies.

- **Trigger:** High volume of TGS (Ticket Granting Service) requests.
- **Signature:** The requests utilized **RC4 (0x17)** encryption, a legacy cipher suite preferred by attackers for its vulnerability to offline brute-force attacks. Standard operations in this environment utilize AES.

2.2 Indicators of Compromise (IoCs)

Forensic analysis of the SecurityEvent logs identified the following artifacts:

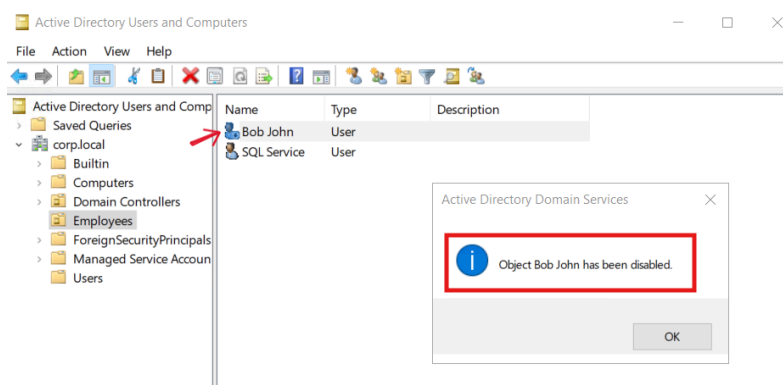| Artifact	Details
Event ID	4769 (A Kerberos service ticket was requested)
Target Service	MSSQL/server-sql.corp.local
Compromised User	bob.john (Source of the request)
Attacker IP	10.0.2.4 (Internal Subnet)
Encryption Type	0x17 (RC4-HMAC)

2.3 Forensic Evidence

The following SIEM log entry confirms the request for a vulnerable ticket type, indicating the use of tools such as Rubeus or Impacket.

the Microsoft Sentinel query results highlighting the malicious TGS request

2.4 Root Cause Analysis

Post-incident investigation on the Domain Controller revealed that the sql-service account had a Service Principal Name (SPN) manually registered but lacked the security controls required for high-privilege accounts (e.g., Managed Service Account status).

2.5 MITRE ATT&CK Mapping

The observed activity aligns with the following techniques within the MITRE ATT&CK framework:

Tactic	Technique ID	Technique Name	Description
Credential Access	T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting	Adversary requested RC4 encrypted TGS tickets for service accounts.
Discovery	T1087.002	Account Discovery: Domain Account	Adversary enumerated user accounts to identify SPN targets.
Defense Evasion	T1078	Valid Accounts: Domain Accounts	Adversary used compromised credentials (bob.john) to interact with the Domain Controller.

3. Containment, Eradication, Recovery & Hardening
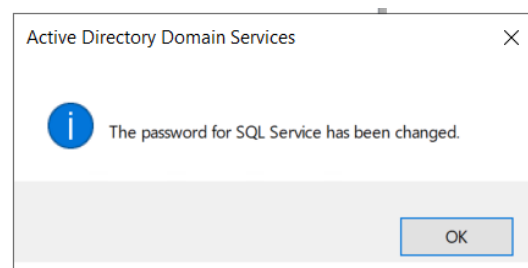
3.1 Containment Actions

Upon verification of the alert, the user account used to initiate the request (bob.john) was disabled in Active Directory to prevent further reconnaissance or lateral movement.

bob.john account disabled

3.2 Eradication & Recovery

To make the stolen ticket hash invalid to the attacker, the password for the sql-service account was changed immediately. This action renders the stolen hash unusable for future authentication attempts, as the extracted hash corresponds to the old password.
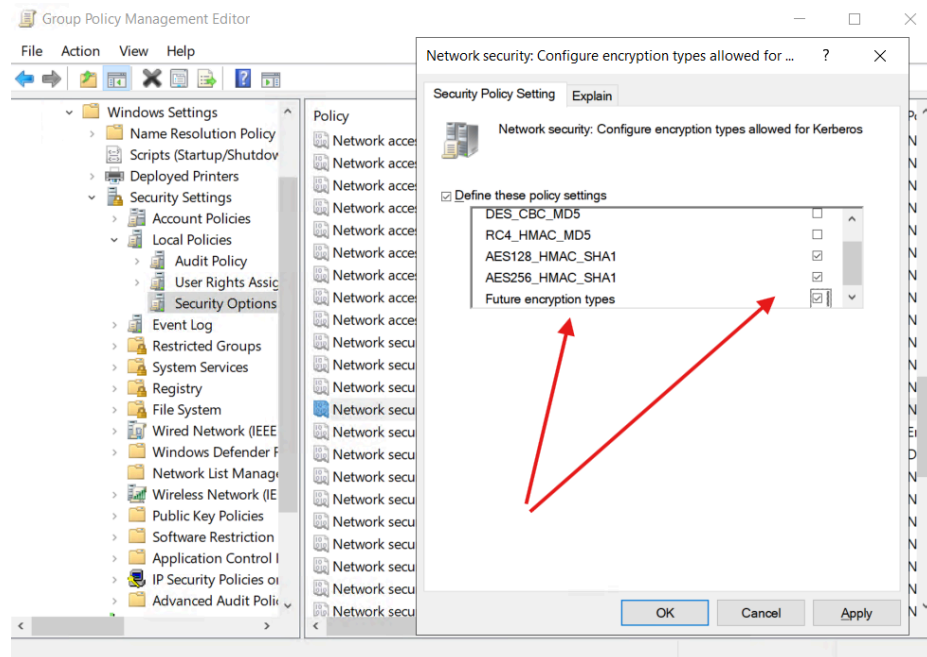

sql.service password changed

3.3 Hardening

To close the vulnerability permanently, the **Default Domain Policy** was updated. I explicitly configured the "Network security: Configure encryption types allowed for Kerberos" setting to **disable RC4_HMAC_MD5** and enforce **AES128/AES256**. This

forces attackers to request AES-encrypted tickets, which are significantly harder to crack offline.

Group Policy configuration enforcing strong encryption standards

4. Recommendations & Hardening

To improve the security posture and prevent future Kerberoasting attempts, the following actions are recommended:

1. **Implement gMSA:** Migrate legacy service accounts to **Group Managed Service Accounts (gMSA)**. This ensures automated, complex password management (120+ characters), making offline cracking virtually impossible.
2. **Password Policy Enforcement:** Ensure all non-gMSA service accounts utilize strong passwords to resist dictionary attacks.
3. **Security Awareness & Phishing Simulations:** Since the attack vector relied on initial access via a compromised standard user account (bob.john), it is critical to conduct regular **Security Awareness Training** and **Phishing Simulation campaigns** to educate employees on the dangers of phishing.