Mega Hacking

Name: Alen Mulangan Davi

Student ID: 10332934

Second Student Name: Antony Jude John

Student ID: 10326739

Due Date: 12/7/2025

Defensive Mitigation Against Kerberoasting

Reset the Service Account Password

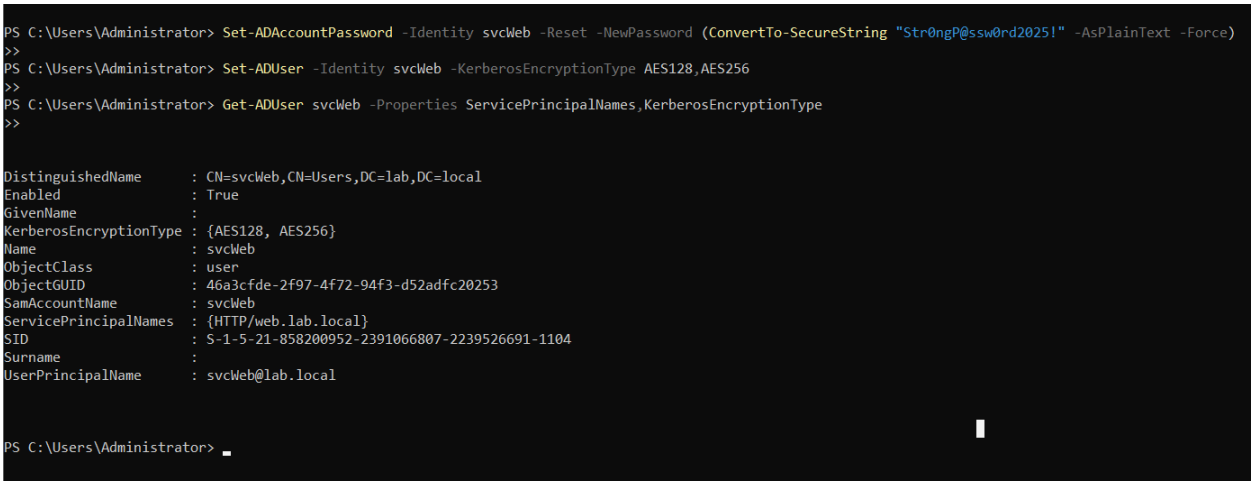
- On the Domain Controller, I opened **PowerShell** as Administrator.
- I reset the password for the vulnerable service account `svcWeb` to a strong value

Enforce Strong Kerberos Encryption

I disabled RC4 and enforced AES encryption only for the account

Verify Account Settings

I confirmed the account now uses AES encryption



Validate Mitigation from Kali

I re-ran the attack from Kali

Short Description of What I Did

In this lab, I set up a Windows Active Directory with a Domain Controller, a Windows 11 computer, and a Kali Linux machine for testing. I made a weak service account called svcWeb and used a Kerberoasting attack with tools like Impacket and John the Ripper to get and break its Kerberos ticket. Once I got the password (Winter2023!), I took steps to improve security by changing the password and using AES encryption to stop old-style ticket cracking. I checked the fix by running the attack again and saw that it didn't work anymore.