

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

```
PS C:\Users\Administrator> Set-ADAccountPassword -Identity svcWeb -Reset -NewPassword (ConvertTo-SecureString "Str0ngP@ssw0rd2025!" -AsPlainText -Force)
>>
PS C:\Users\Administrator> Set-ADUser -Identity svcWeb -KerberosEncryptionType AES128,AES256
>>
PS C:\Users\Administrator> Get-ADUser svcWeb -Properties ServicePrincipalNames,KerberosEncryptionType
>>

DistinguishedName      : CN=svcWeb,CN=Users,DC=lab,DC=local
Enabled                 : True
GivenName               :
KerberosEncryptionType : {AES128, AES256}
Name                   : svcWeb
ObjectClass              : user
ObjectGUID              : 46a3cfde-2f97-4f72-94f3-d52adfc20253
SamAccountName          : svcWeb
ServicePrincipalNames   : {HTTP/web.lab.local}
SID                     : S-1-5-21-858200952-2391066807-2239526691-1104
Surname                 :
UserPrincipalName       : svcWeb@lab.local

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

Validate Mitigation from Kali

I re-ran the attack from Kali

```
(root@kali)-[/home/kali]
# python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py lab.local/jdoe:UserPass123! -dc-ip 192.168.234.150 -request -outputfile tgs_hashes_new.txt
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name      MemberOf  PasswordLastSet      LastLogon  Delegation
-----
HTTP/web.lab.local    svcWeb      

2025-12-07 11:48:46.274536  <never>

[-] CCache file is not found. Skipping...

(root@kali)-[/home/kali]
# john --format=krb5tgs --wordlist=/usr/share/wordlists/rockyou.txt tgs_hashes_new.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

(root@kali)-[/home/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.