34-Additional AD Auditing Techniques

in this topic we will use tool for AD Auditing Techniques

1-Creating an AD Snapshot with Active Directory Explorer

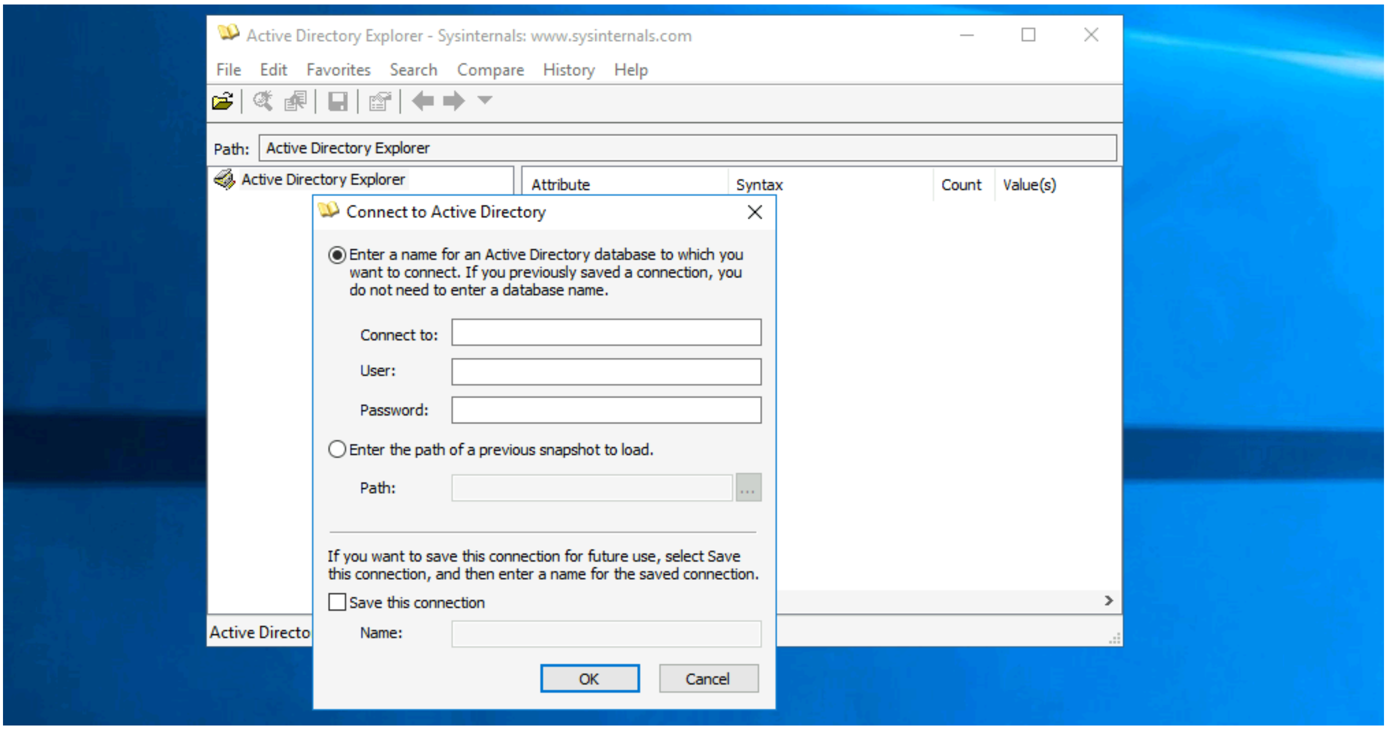
 AD Explorer: https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer[](https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer) is part of the Sysinternal Suite and is described as:

"An advanced Active Directory (AD) viewer and editor. You can use AD Explorer to navigate an AD database easily, define favorite locations, view object properties, and attributes without opening dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that you can save and re-execute."

AD Explorer can also be used to save snapshots of an AD database for offline viewing and comparison. We can take a snapshot of AD at a point in time and explore it later, during the reporting phase, as you would explore any other database. It can also be used to perform a before and after comparison of AD to uncover changes in objects, attributes, and security permissions.

When we first load the tool, we are prompted for login credentials or to load a previous snapshot. We can log in with any valid domain user.

Logging in with AD Explorer



Path: Active Directory Explorer

Connect to Active Directory

● Enter a name for an Active Directory database to which you want to connect. If you previously saved a connection, you do not need to enter a database name.

Connect to:

User:

Password:

○ Enter the path of a previous snapshot to load.

Path:

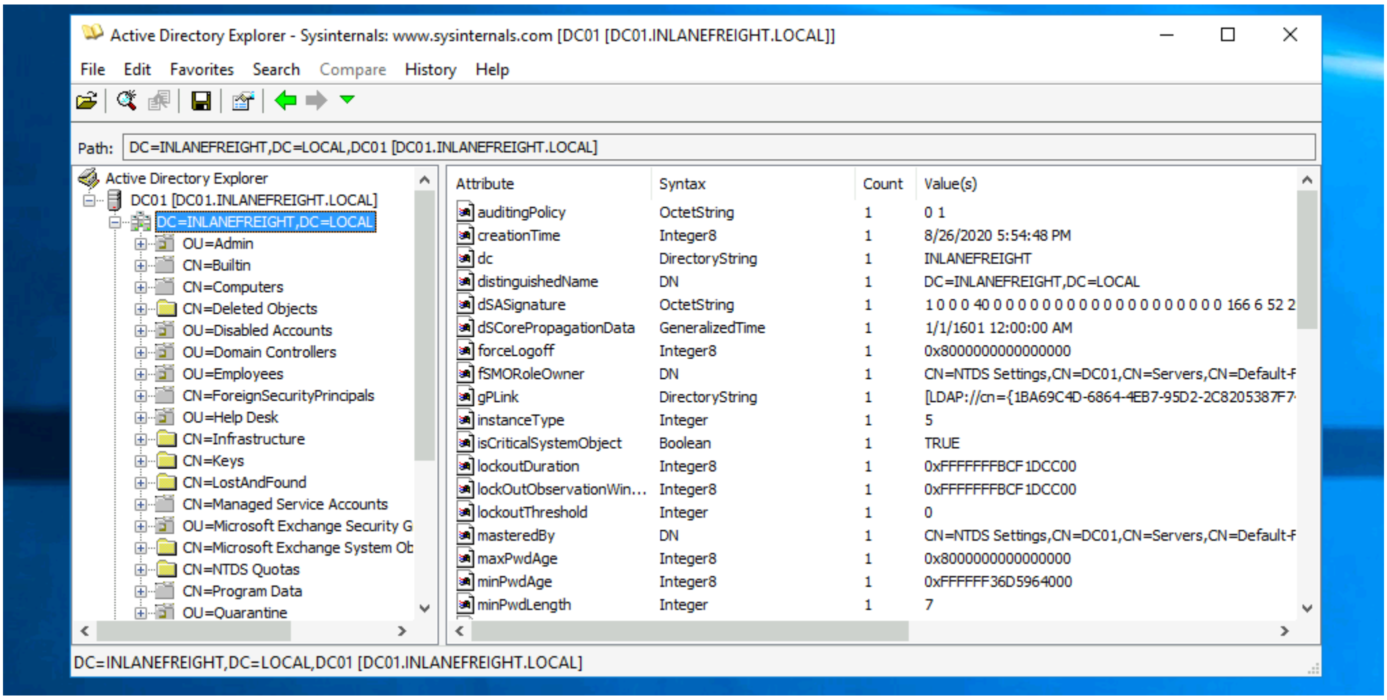
If you want to save this connection for future use, select Save this connection, and then enter a name for the saved connection.

□ Save this connection

Name:

Once logged in, we can freely browse AD and view information about all objects.

Browsing AD with AD Explorer



Active Directory Explorer - Sysinternals: www.sysinternals.com [DC01 [DC01.INLANEFREIGHT.LOCAL]]

Path: DC=INLANEFREIGHT,DC=LOCAL,DC01 [DC01.INLANEFREIGHT.LOCAL]

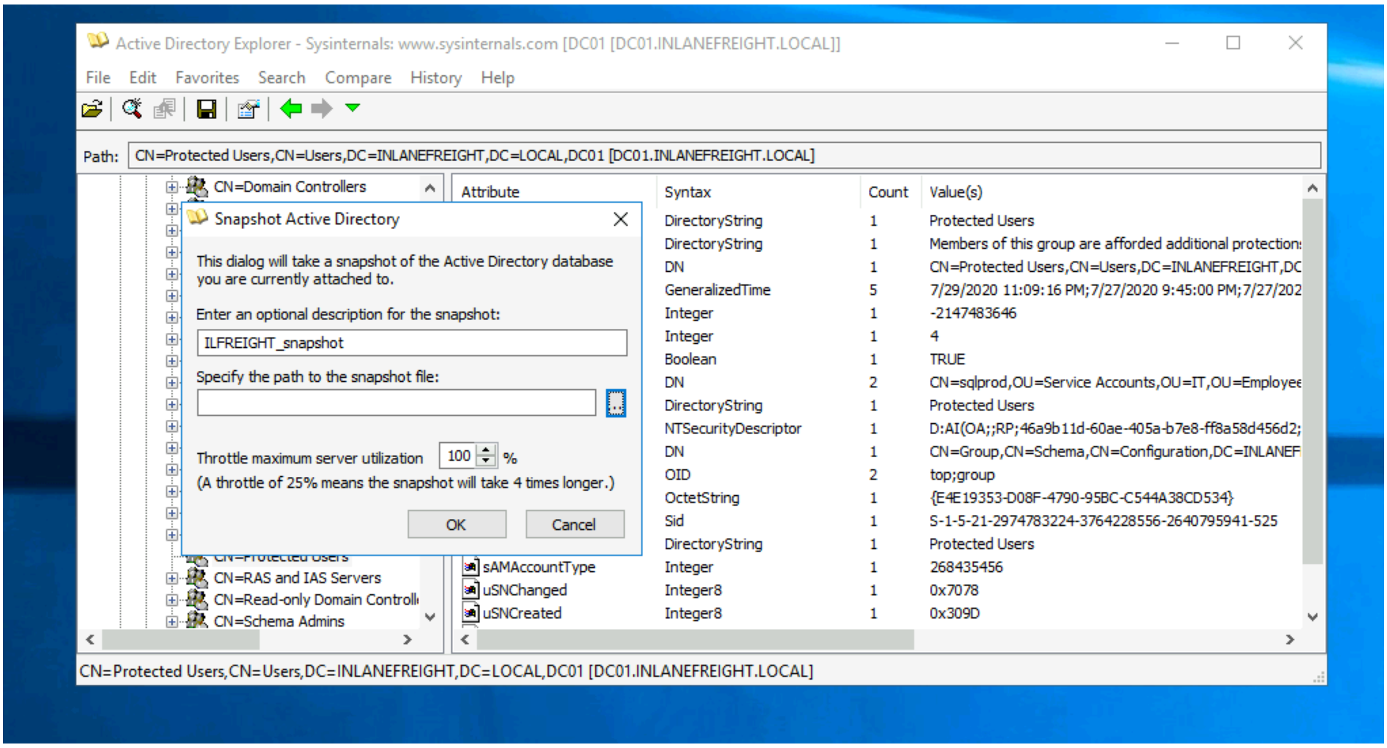
- Active Directory Explorer
  - DC01 [DC01.INLANEFREIGHT.LOCAL]
    - DC=INLANEFREIGHT,DC=LOCAL
      - OU=Admin
      - CN=Builtin
      - CN=Computers
      - CN=Deleted Objects
      - OU=Disabled Accounts
      - OU=Domain Controllers
      - OU=Employees
      - CN=ForeignSecurityPrincipals
      - OU=Help Desk
      - CN=Infrastructure
      - CN=Keys
      - CN=LostAndFound
      - CN=Managed Service Accounts
      - OU=Microsoft Exchange Security G
      - CN=Microsoft Exchange System Ob
      - CN=NTDS Quotas
      - CN=Program Data
      - OU=Quarantine

Attribute	Syntax	Count	Value(s)
auditingPolicy	OctetString	1	0 1
creationTime	Integer8	1	8/26/2020 5:54:48 PM
dc	DirectoryString	1	INLANEFREIGHT
distinguishedName	DN	1	DC=INLANEFREIGHT,DC=LOCAL
dSASignature	OctetString	1	1 0 0 0 40 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 166 6 52 2
dSCorePropagationData	GeneralizedTime	1	1/1/1601 12:00:00 AM
forceLogoff	Integer8	1	0x8000000000000000
fSMORoleOwner	DN	1	CN=NTDS Settings,CN=DC01,CN=Servers,CN=Default-F
gPLink	DirectoryString	1	[LDAP://cn={1BA69C4D-6864-4EB7-95D2-2C8205387F7
instanceType	Integer	1	5
isCriticalSystemObject	Boolean	1	TRUE
lockoutDuration	Integer8	1	0xFFFFFFFBCF1DCC00
lockOutObservationWin...	Integer8	1	0xFFFFFFFBCF1DCC00
lockoutThreshold	Integer	1	0
masteredBy	DN	1	CN=NTDS Settings,CN=DC01,CN=Servers,CN=Default-F
maxPwdAge	Integer8	1	0x8000000000000000
minPwdAge	Integer8	1	0xFFFFFF36D5964000
minPwdLength	Integer	1	7

DC=INLANEFREIGHT,DC=LOCAL,DC01 [DC01.INLANEFREIGHT.LOCAL]

To take a snapshot of AD, go to File --> `Create Snapshot` and enter a name for the snapshot. Once it is complete, we can move it offline for further analysis.

Creating a Snapshot of AD with AD Explorer



Active Directory Explorer - Sysinternals: www.sysinternals.com [DC01 [DC01.INLANEFREIGHT.LOCAL]]

Path: CN=Protected Users,CN=Users,DC=INLANEFREIGHT,DC=LOCAL,DC01 [DC01.INLANEFREIGHT.LOCAL]

- CN=Domain Controllers
- CN=Protected Users
- CN=RAS and IAS Servers
- CN=Read-only Domain Controll
- CN=Schema Admins

Snapshot Active Directory

This dialog will take a snapshot of the Active Directory database you are currently attached to.

Enter an optional description for the snapshot:

ILFREIGHT_snapshot

Specify the path to the snapshot file:

Throttle maximum server utilization 100 %

(A throttle of 25% means the snapshot will take 4 times longer.)

Attribute	Syntax	Count	Value(s)
	DirectoryString	1	Protected Users
	DirectoryString	1	Members of this group are afforded additional protection:
	DN	1	CN=Protected Users,CN=Users,DC=INLANEFREIGHT,DC
	GeneralizedTime	5	7/29/2020 11:09:16 PM;7/27/2020 9:45:00 PM;7/27/202
	Integer	1	-2147483646
	Integer	1	4
	Boolean	1	TRUE
	DN	2	CN=sqlprod,OU=Service Accounts,OU=IT,OU=Employee
	DirectoryString	1	Protected Users
	NTSecurityDescriptor	1	D:AI(OA;;RP;46a9b11d-60ae-405a-b7e8-ff8a58d456d2;
	DN	1	CN=Group,CN=Schema,CN=Configuration,DC=INLANEF
	OID	2	top;group
	OctetString	1	{E4E19353-D08F-4790-95BC-C544A38CD534}
	Sid	1	S-1-5-21-2974783224-3764228556-2640795941-525
	DirectoryString	1	Protected Users
sAMAccountType	Integer	1	268435456
uSNChanged	Integer8	1	0x7078
uSNCreated	Integer8	1	0x309D

CN=Protected Users,CN=Users,DC=INLANEFREIGHT,DC=LOCAL,DC01 [DC01.INLANEFREIGHT.LOCAL]

PingCastle

PingCastle: https://www.pingcastle.com/documentation/[](https://www.pingcastle.com/documentation/) is a powerful tool that evaluates the security posture of an AD environment and provides us the results in several different maps and graphs. Thinking about security for a second, if you do not have an active inventory of the hosts in your enterprise, PingCastle can be a great resource to help you gather one in a nice user-readable map of the domain. PingCastle is different from tools such as PowerView and BloodHound because, aside from **providing us with enumeration data that can inform our attacks, it also provides a detailed report of the target domain's security level using a methodology based on a risk assessment/maturity framework**. The scoring shown in the report is based on the Capability Maturity Model Integration (CMMI). For a quick look at the help context provided, you can issue the `--help` switch in cmd-prompt.

Viewing the PingCastle Help Menu

```
C:\htb> PingCastle.exe --help

switch:
  --help              : display this message
  --interactive       : force the interactive mode
  --log               : generate a log file
  --log-console       : add log to the console
  --log-samba <option>: enable samba login (example: 10)

Common options when connecting to the AD
  --server <server>   : use this server (default: current domain controller)
                        the special value * or *.forest do the healthcheck
for all domains
  --port <port>       : the port to use for ADWS or LDAP (default: 9389 or
389)
  --user <user>       : use this user (default: integrated authentication)
  --password <pass>   : use this password (default: asked on a secure
prompt)
  --protocol <proto>  : selection the protocol to use among LDAP or ADWS
(fastest)
                      : ADWSThenLDAP (default), ADWSOnly, LDAPOnly,
LDAPThenADWS

<SNIP>
```

Running PingCastle

To run PingCastle, we can call the executable by typing `PingCastle.exe` into our CMD or PowerShell window or by clicking on the executable, and it will drop us into interactive mode, presenting us with a menu of options inside the `Terminal User Interface` (`TUI`).

PingCastle Interactive TUI

```
|:.      PingCastle (Version 2.10.1.0     1/19/2022 8:12:02 AM)
|  #:.   Get Active Directory Security at 80% in 20% of the time
# @@  >  End of support: 7/31/2023
| @@@:
: .#                                 Vincent LE TOUX
(contact@pingcastle.com)
  .:       twitter: @mysmartlogon
https://www.pingcastle.com
What do you want to do?
=======================
Using interactive mode.
Do not forget that there are other command line switches like --help that
you can use
  1-healthcheck-Score the risk of a domain
  2-conso      -Aggregate multiple reports into a single one
  3-carto      -Build a map of all interconnected domains
  4-scanner    -Perform specific security checks on workstations
  5-export     -Export users or computers
  6-advanced   -Open the advanced menu
  0-Exit
==============================
This is the main functionnality of PingCastle. In a matter of minutes, it
produces a report which will give you an overview of your Active Directory
security. This report can be generated on other domains by using the
existing trust links.
```

The default option is the `healthcheck` run, which will establish a baseline overview of the domain, and provide us with pertinent information dealing with misconfigurations and vulnerabilities. Even better, PingCastle can report recent vulnerability susceptibility, our shares, trusts, the delegation of permissions, and much more about our user and computer states. Under the Scanner option, we can find most of these checks.

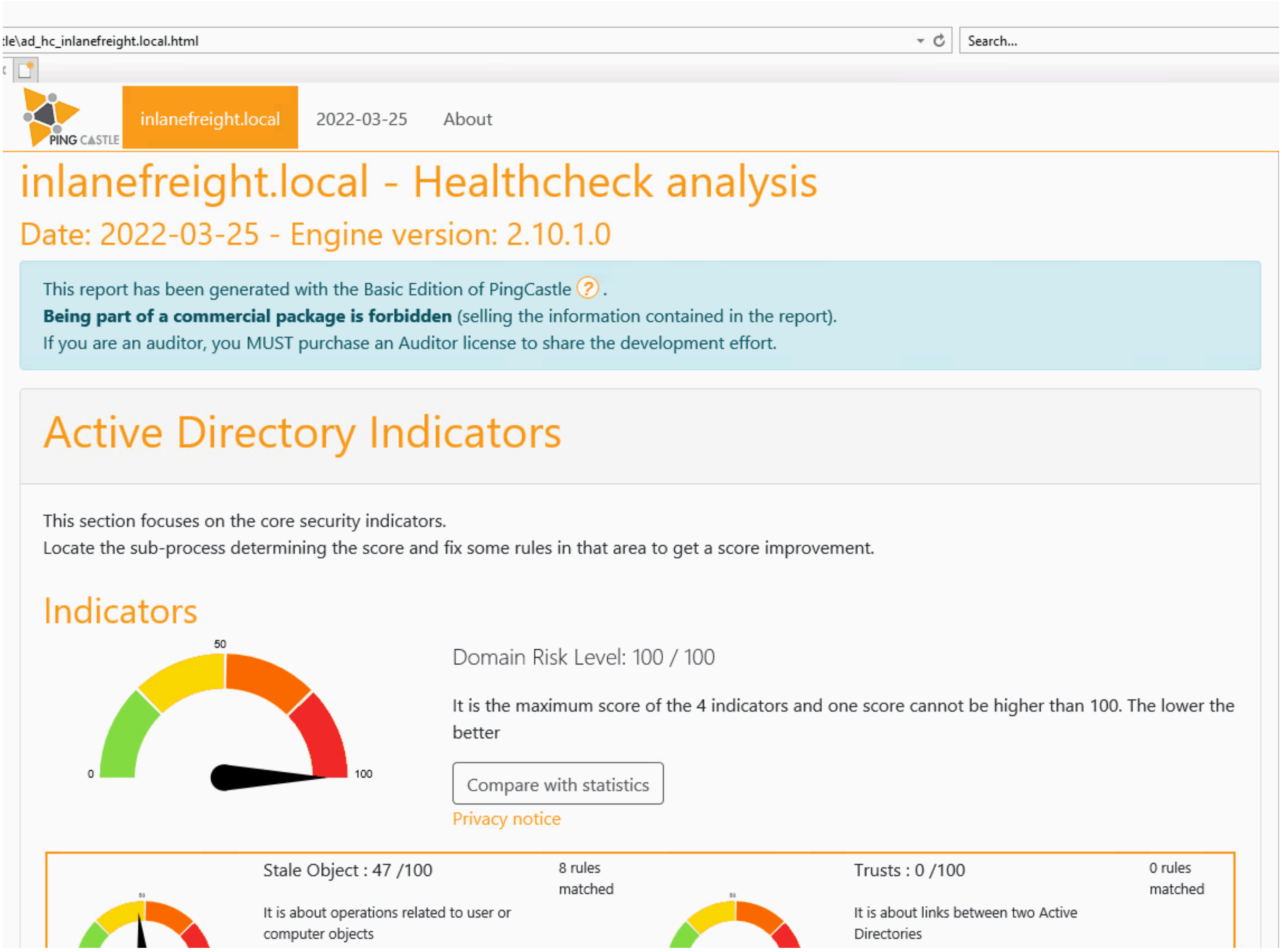
Scanner Options

```
|:.      PingCastle (Version 2.10.1.0     1/19/2022 8:12:02 AM)
|  #:.   Get Active Directory Security at 80% in 20% of the time
# @@  >  End of support: 7/31/2023
| @@@:
: .#                                 Vincent LE TOUX
(contact@pingcastle.com)
  .:       twitter: @mysmartlogon
https://www.pingcastle.com
Select a scanner
================
What scanner whould you like to run ?
WARNING: Checking a lot of workstations may raise security alerts.
  1-aclcheck                                                  9-oxidbindings
  2-antivirus                                                 a-remote
  3-computerversion                                           b-share
  4-foreignusers                                              c-smb
  5-laps_bitlocker                                            d-
smb3querynetwork
  6-localadmin                                                e-spooler
  7-nullsession                                               f-startup
  8-nullsession-trust                                         g-zerologon
  0-Exit
==============================
Check authorization related to users or groups. Default to everyone,
authenticated users and domain users
```

Now that we understand how it works and how to start scans, let's view the report.

Viewing The Report

Throughout the report, there are sections such as domain, user, group, and trust information and a specific table calling out "anomalies" or issues that may require immediate attention. We will also be presented with the domain's overall risk score.



inlanefreight.local - Healthcheck analysis

Date: 2022-03-25 - Engine version: 2.10.1.0

This report has been generated with the Basic Edition of PingCastle ? .
Being part of a commercial package is forbidden (selling the information contained in the report).
If you are an auditor, you MUST purchase an Auditor license to share the development effort.

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: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice

Stale Object : 47 /100 — 8 rules matched

It is about operations related to user or computer objects

Trusts : 0 /100 — 0 rules matched

It is about links between two Active Directories

3-Group3r

Group3r is a tool purpose-built to find vulnerabilities in Active Directory associated Group Policy. Group3r must be run from a domain-joined host with a domain user (it does not need to be an administrator), or in the context of a domain user (i.e., using `runas /netonly`).

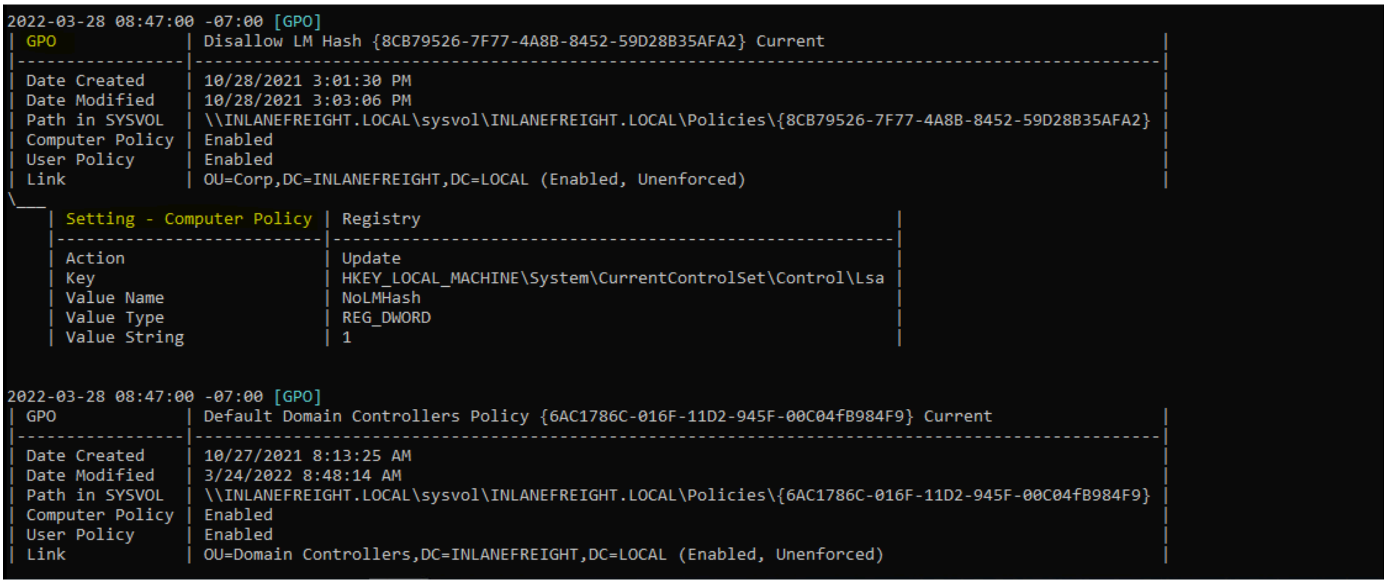
Group3r Basic Usage

```
C:\htb> group3r.exe -f <filepath-name.log>
```

When running Group3r, we must specify the `-s` or the `-f` flag. These will specify whether to send results to stdout (-s), or to the file we want to send the results to (-f). For more options and usage information, utilize the `-h` flag, or check out the usage info at the link above.

Below is an example of starting Group3r.

Reading Output

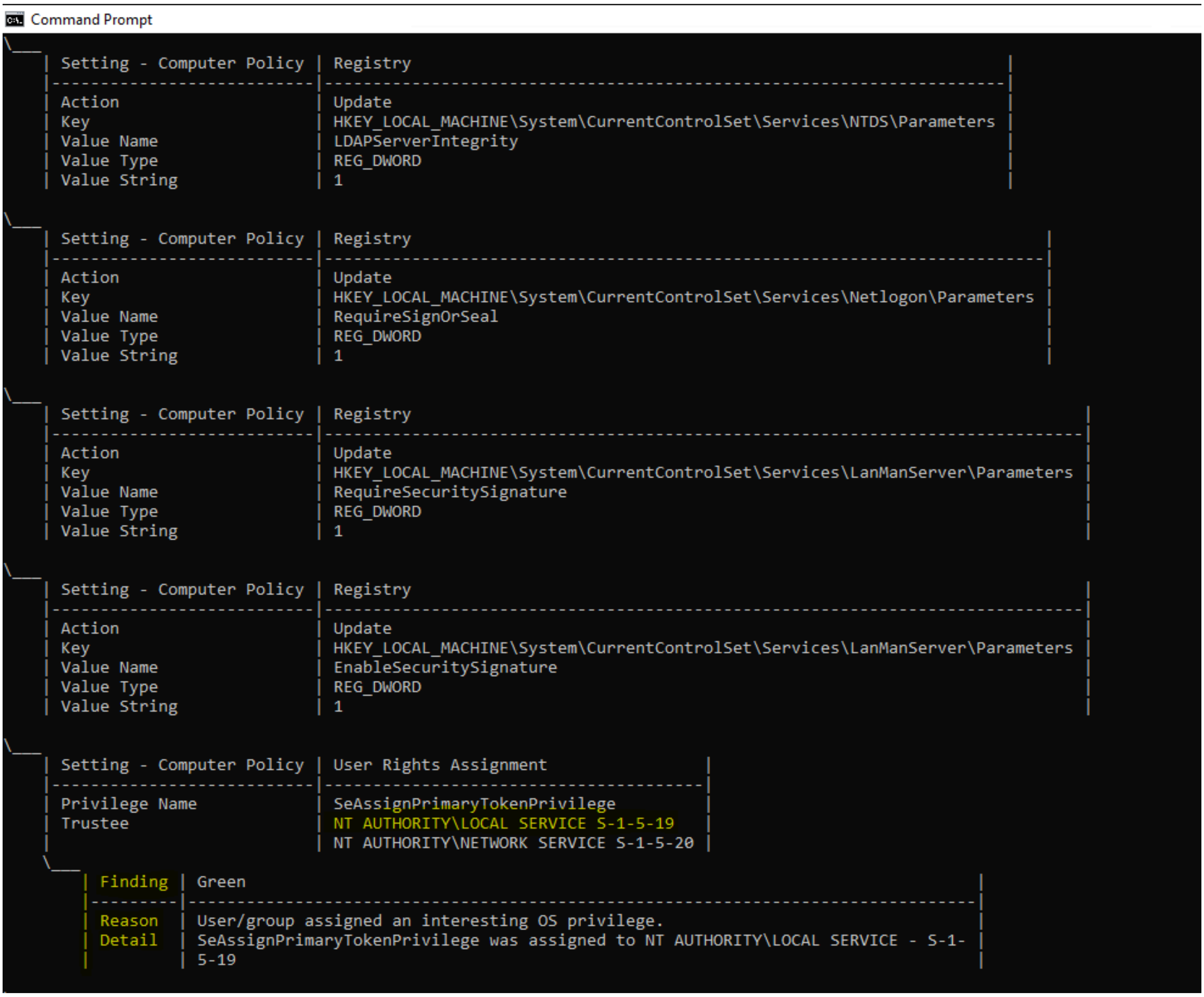


```
2022-03-28 08:47:00 -07:00 [GPO]
| GPO              | Disallow LM Hash {8CB79526-7F77-4A8B-8452-59D28B35AFA2} Current                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------|
| Date Created     | 10/28/2021 3:01:30 PM                                                                                                 |
| Date Modified    | 10/28/2021 3:03:06 PM                                                                                                 |
| Path in SYSVOL   | \\INLANEFREIGHT.LOCAL\sysvol\INLANEFREIGHT.LOCAL\Policies\{8CB79526-7F77-4A8B-8452-59D28B35AFA2} |
| Computer Policy  | Enabled                                                                                                               |
| User Policy      | Enabled                                                                                                               |
| Link             | OU=Corp,DC=INLANEFREIGHT,DC=LOCAL (Enabled, Unenforced)                                                               |
\___
    | Setting - Computer Policy | Registry                                                 |
    |---------------------------|----------------------------------------------------------|
    | Action                    | Update                                                   |
    | Key                       | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa |
    | Value Name                | NoLMHash                                                 |
    | Value Type                | REG_DWORD                                                |
    | Value String              | 1                                                        |


2022-03-28 08:47:00 -07:00 [GPO]
| GPO              | Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9} Current                                      |
|------------------|-----------------------------------------------------------------------------------------------------------------------|
| Date Created     | 10/27/2021 8:13:25 AM                                                                                                 |
| Date Modified    | 3/24/2022 8:48:14 AM                                                                                                  |
| Path in SYSVOL   | \\INLANEFREIGHT.LOCAL\sysvol\INLANEFREIGHT.LOCAL\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9} |
| Computer Policy  | Enabled                                                                                                               |
| User Policy      | Enabled                                                                                                               |
| Link             | OU=Domain Controllers,DC=INLANEFREIGHT,DC=LOCAL (Enabled, Unenforced)                                                 |
```

When reading the output from Group3r, each indentation is a different level, so no indent will be the GPO, one indent will be policy settings, and another will be findings in those settings. Below we will take a look at the output shown from a finding.

Group3r Finding



Command Prompt

```
\___
    | Setting - Computer Policy | Registry                                                               |
    |---------------------------|------------------------------------------------------------------------|
    | Action                    | Update                                                                 |
    | Key                       | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters |
    | Value Name                | LDAPServerIntegrity                                                    |
    | Value Type                | REG_DWORD                                                              |
    | Value String              | 1                                                                      |

\___
    | Setting - Computer Policy | Registry                                                                   |
    |---------------------------|----------------------------------------------------------------------------|
    | Action                    | Update                                                                     |
    | Key                       | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters |
    | Value Name                | RequireSignOrSeal                                                          |
    | Value Type                | REG_DWORD                                                                  |
    | Value String              | 1                                                                          |

\___
    | Setting - Computer Policy | Registry                                                                       |
    |---------------------------|--------------------------------------------------------------------------------|
    | Action                    | Update                                                                         |
    | Key                       | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters |
    | Value Name                | RequireSecuritySignature                                                       |
    | Value Type                | REG_DWORD                                                                      |
    | Value String              | 1                                                                              |

\___
    | Setting - Computer Policy | Registry                                                                       |
    |---------------------------|--------------------------------------------------------------------------------|
    | Action                    | Update                                                                         |
    | Key                       | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters |
    | Value Name                | EnableSecuritySignature                                                        |
    | Value Type                | REG_DWORD                                                                      |
    | Value String              | 1                                                                              |

\___
    | Setting - Computer Policy | User Rights Assignment              |
    |---------------------------|-------------------------------------|
    | Privilege Name            | SeAssignPrimaryTokenPrivilege       |
    | Trustee                   | NT AUTHORITY\LOCAL SERVICE S-1-5-19 |
    |                           | NT AUTHORITY\NETWORK SERVICE S-1-5-20 |
    \___
        | Finding | Green                                                                    |
        |---------|--------------------------------------------------------------------------|
        | Reason  | User/group assigned an interesting OS privilege.                         |
        | Detail  | SeAssignPrimaryTokenPrivilege was assigned to NT AUTHORITY\LOCAL SERVICE - S-1- |
        |         | 5-19                                                                     |
```

4-ADRecon

Finally, there are several other tools out there that are useful for gathering a large amount of data from AD at once. In an assessment where stealth is not required, it is also worth running a tool like ADRecon: https://github.com/adrecon/ADRecon[](https://github.com/adrecon/ADRecon) and analyzing the results, just in case all of our enumeration missed something minor that may be useful to us or worth pointing out to our client.

Running ADRecon

```
PS C:\htb> .\ADRecon.ps1

[*] ADRecon v1.1 by Prashant Mahajan (@prashant3535)
[*] Running on INLANEFREIGHT.LOCAL\MS01 - Member Server
[*] Commencing - 03/28/2022 09:24:58
[-] Domain
[-] Forest
[-] Trusts
[-] Sites
[-] Subnets
[-] SchemaHistory - May take some time
[-] Default Password Policy
[-] Fine Grained Password Policy - May need a Privileged Account
[-] Domain Controllers
[-] Users and SPNs - May take some time
[-] PasswordAttributes - Experimental
[-] Groups and Membership Changes - May take some time
[-] Group Memberships - May take some time
[-] OrganizationalUnits (OUs)
[-] GPOs
[-] gPLinks - Scope of Management (SOM)
[-] DNS Zones and Records
[-] Printers
[-] Computers and SPNs - May take some time
[-] LAPS - Needs Privileged Account
[-] BitLocker Recovery Keys - Needs Privileged Account
[-] GPOReport - May take some time
[*] Total Execution Time (mins): 11.05
[*] Output Directory: C:\Tools\ADRecon-Report-20220328092458
```

Once done, ADRecon will drop a report for us in a new folder under the directory we executed from. We can see an example of the results in the terminal below. You will get a report in HTML format and a folder with CSV results. When generating the report, it should be noted that the program Excel needs to be installed, or the script will not automatically generate the report in that manner; it will just leave you with the .csv files. If you want output for Group Policy, you need to ensure the host you run from has the `GroupPolicy` PowerShell module installed. We can go back later and generate the Excel report from another host using the `-GenExcel` switch and feeding in the report folder.

Reporting

```
PS C:\htb> ls


    Directory: C:\Tools\ADRecon-Report-20220328092458


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         3/28/2022  12:42 PM                CSV-Files
-a----         3/28/2022  12:42 PM        2758736 GPO-Report.html
-a----         3/28/2022  12:42 PM         392780 GPO-Report.xml
```