7. Note Formatting

As your note repository grows, it is essential to maintain a consistent style throughout all your notes. This makes referencing older notes easier, as you already know where to find the information without having to read the entire note.

In this section, my aim is to teach you how to keep your vault consistent while saving tons of time and adding longevity to your notes.

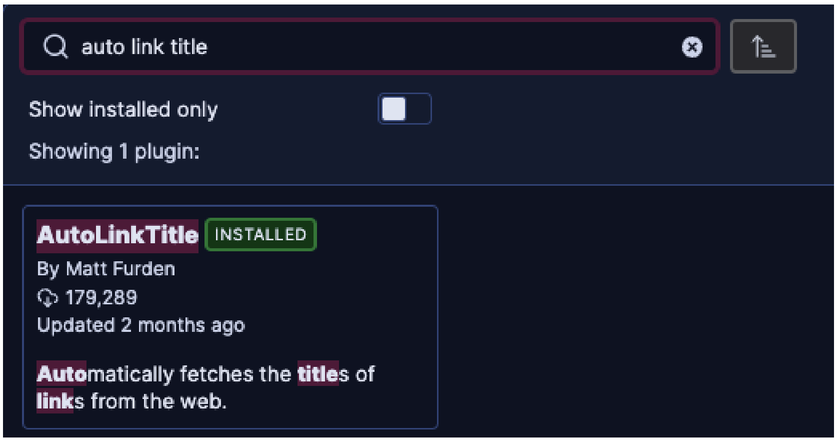
7.1 Plugins Needed for This Methodology

For this methodology, you will need the following plugin(s):

1. **Auto Link Title**: Auto Link Title automatically grabs a URL's title from the website's HTML title upon pasting it in your note. It can also scan your note for bare URLs and rename them appropriately. This is a big time saver.
2. **Footnote Shortcut**: Footnote Shortcut automates part of the footnote creation process. This is very useful if you prefer to cite your sources using footnotes instead of a dedicated "Resources" section. It can also be helpful if you are working on your own content and would like to add footnotes for citation purposes without using your mouse. I have used this plugin extensively during the creation of this course.
3. **Linter**: Linter is a formatting plugin which I mentioned in the 6. Metadata section of this course. It has a feature that scans your notes and is capable of fixing whitespace issues, metadata, and style discrepancies. It is a game-changer plugin that you will use every day.
4. **Markmind**: Markmind enables you to create special mindmap notes without leaving Obsidian. This is useful for instances where you need to write a mindmap to visualize concepts.
5. **Note Refactor**: Note Refactor can be used to split a long note into several atomic notes. This is very useful because having long notes with more than one topic can make them harder to read and reference.
6. **Table of Contents**: Table of Contents scans your note and creates a table of contents. This is very useful for reports, which are notes that have to be long. I usually create a table of contents whenever I write exam reports to make it easier for the reader.
7. **Various Complements**: Various Complements has a ton of features, as its name implies. The reason I use it myself is for its auto-correct feature, which resembles that of an IDE. Sometimes when writing notes, you will find yourself writing long and complex names, and this plugin will automatically create suggestions. It also features syntax highlighting, which is very useful for keeping your spelling in check.

7.2 How to Implement This Methodology

Start by installing each of these plugins from the Community Plugins tab.



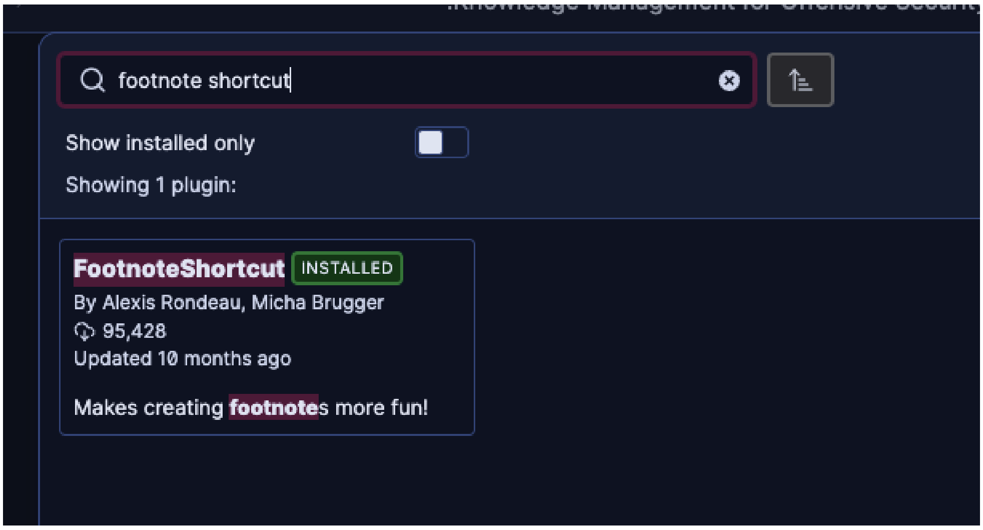
auto link title

Show installed only

Showing 1 plugin:

AutoLinkTitle INSTALLED
By Matt Furden
179,289
Updated 2 months ago

Automatically fetches the titles of links from the web.



:Knowledge Management for Offensive Securit

footnote shortcut

Show installed only

Showing 1 plugin:

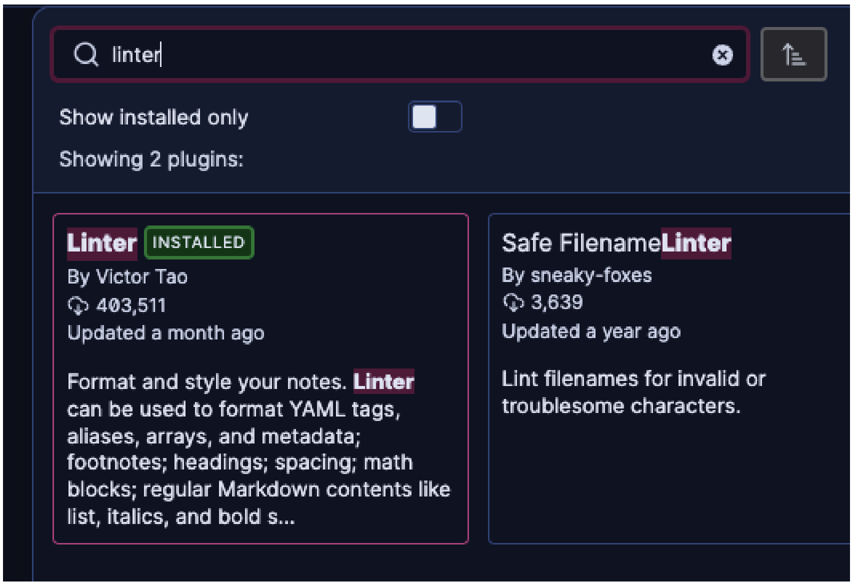
FootnoteShortcut INSTALLED

By Alexis Rondeau, Micha Brugger

95,428

Updated 10 months ago

Makes creating **footnote**s more fun!



linter

Show installed only

Showing 2 plugins:

Linter INSTALLED

By Victor Tao

403,511

Updated a month ago

Format and style your notes. **Linter** can be used to format YAML tags, aliases, arrays, and metadata; footnotes; headings; spacing; math blocks; regular Markdown contents like list, italics, and bold s...

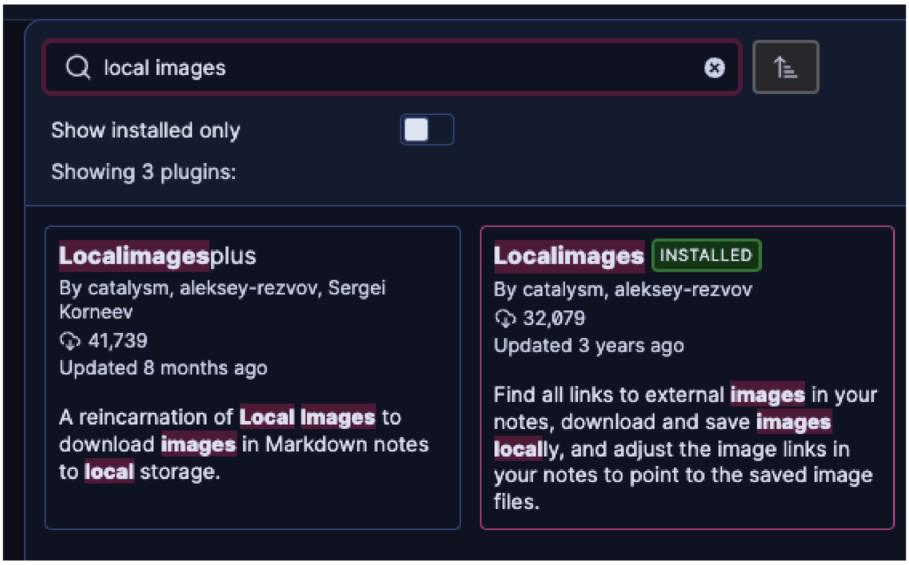
Safe Filename**Linter**

By sneaky-foxes

3,639

Updated a year ago

Lint filenames for invalid or troublesome characters.



local images

Show installed only

Showing 3 plugins:

Localimagesplus

By catalysm, aleksey-rezvov, Sergei Korneev

41,739

Updated 8 months ago

A reincarnation of **Local Images** to download **images** in Markdown notes to **local** storage.

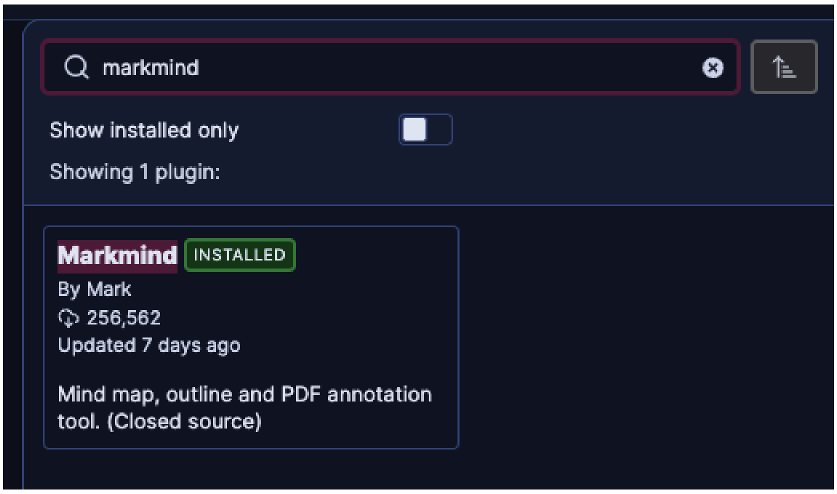
Localimages INSTALLED

By catalysm, aleksey-rezvov

32,079

Updated 3 years ago

Find all links to external **images** in your notes, download and save **images** **local**ly, and adjust the image links in your notes to point to the saved image files.



markmind

Show installed only

Showing 1 plugin:

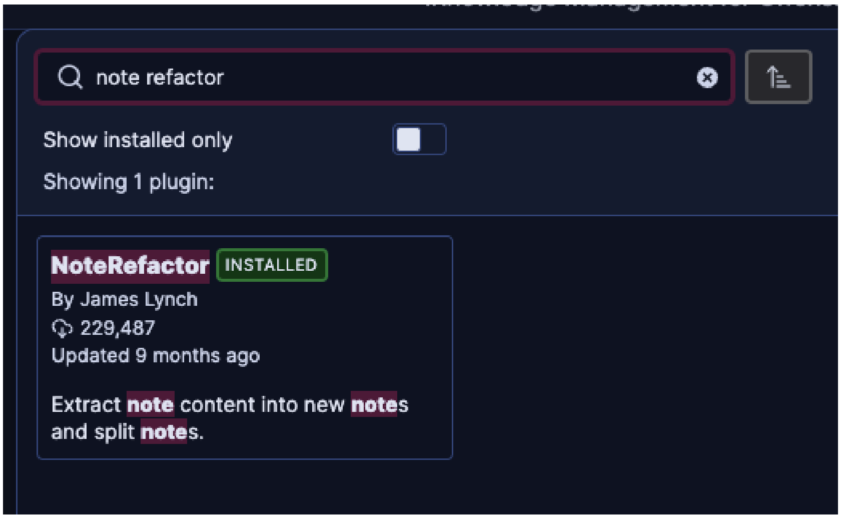
Markmind INSTALLED

By Mark

256,562

Updated 7 days ago

Mind map, outline and PDF annotation tool. (Closed source)



note refactor

Show installed only

Showing 1 plugin:

NoteRefactor INSTALLED

By James Lynch

229,487

Updated 9 months ago

Extract **note** content into new **note**s and split **note**s.

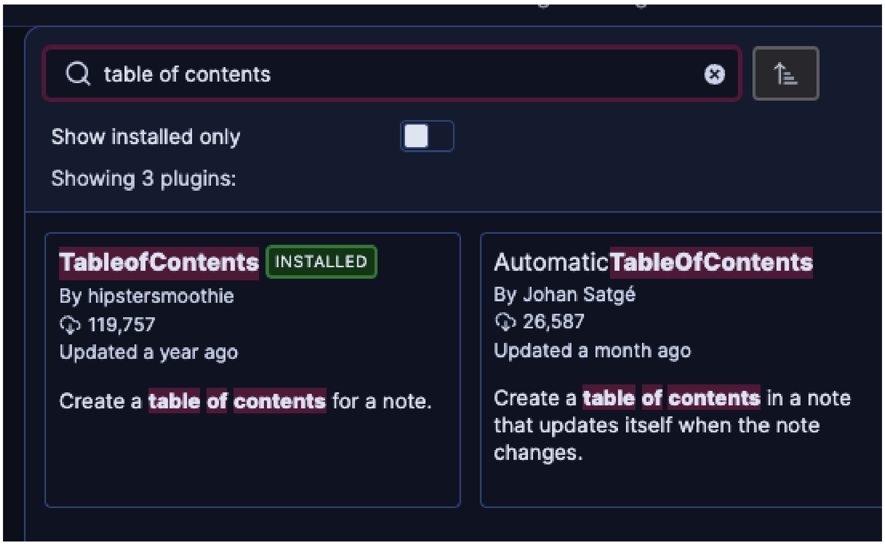


table of contents

Show installed only

Showing 3 plugins:

TableofContents INSTALLED

By hipstersmoothie

119,757

Updated a year ago

Create a **table of contents** for a note.

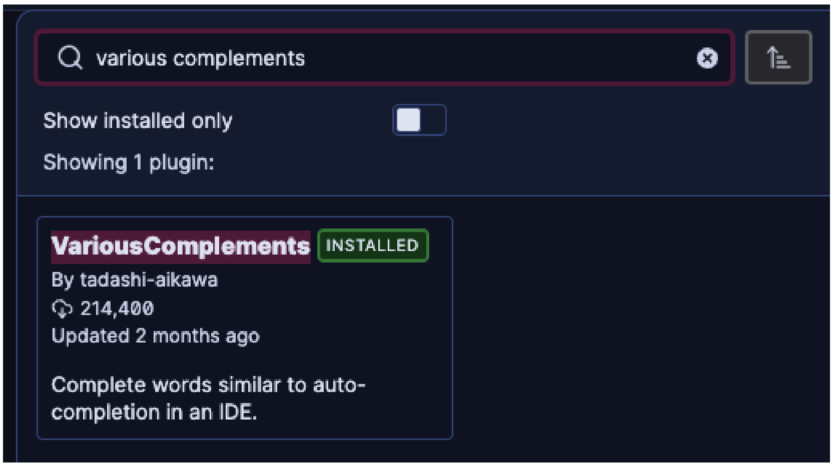
Automatic**TableOfContents**

By Johan Satgé

26,587

Updated a month ago

Create a **table of contents** in a note that updates itself when the note changes.



various complements

Show installed only

Showing 1 plugin:

VariousComplements INSTALLED

By tadashi-aikawa

214,400

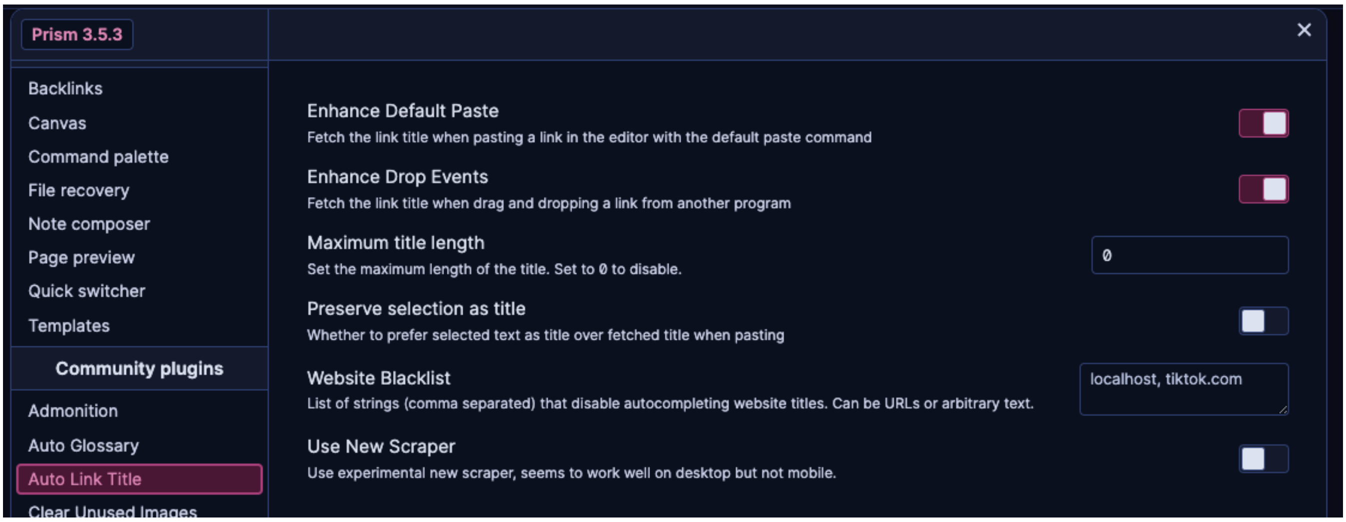
Updated 2 months ago

Complete words similar to auto-completion in an IDE.

7.2.1 Auto Link Title Setup

Remember that you can change the settings for each plugin by opening the settings window and going to the Community Plugins section on the left.

These are my settings:



Enhance Default Paste
Fetch the link title when pasting a link in the editor with the default paste command

Enhance Drop Events
Fetch the link title when drag and dropping a link from another program

Maximum title length
Set the maximum length of the title. Set to 0 to disable.
0

Preserve selection as title
Whether to prefer selected text as title over fetched title when pasting

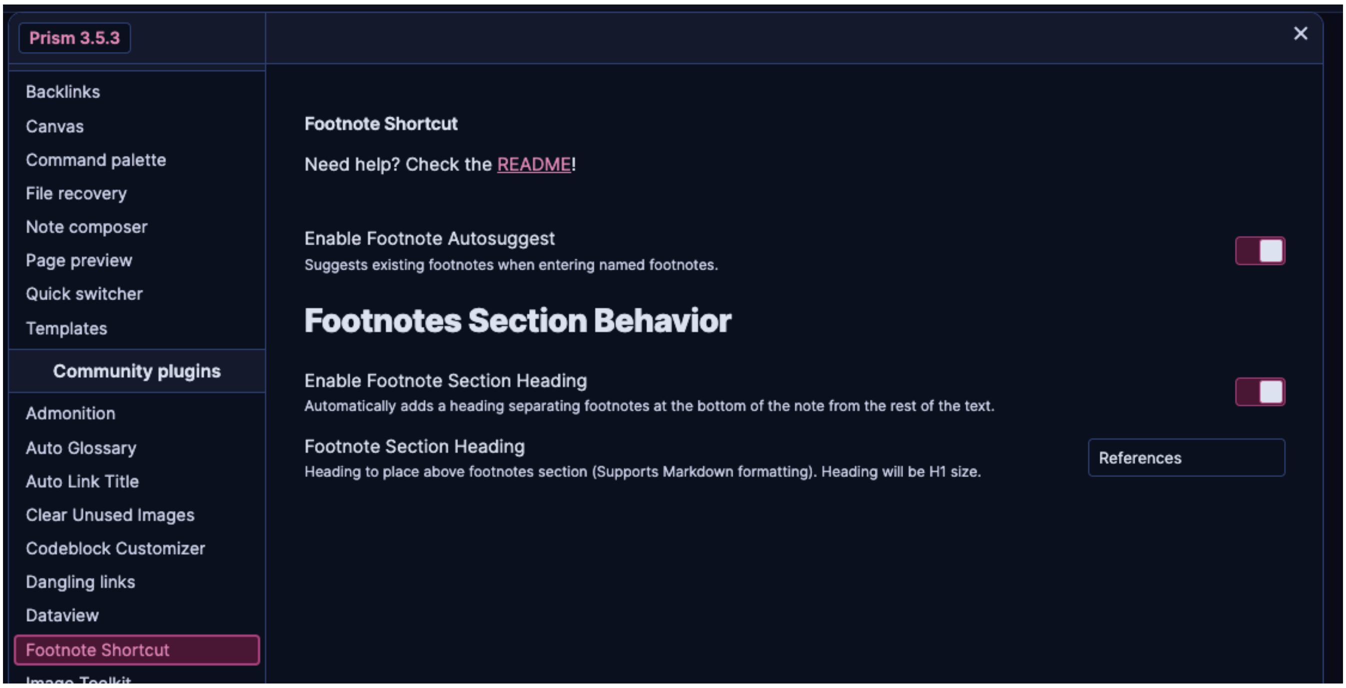
Website Blacklist
List of strings (comma separated) that disable autocompleting website titles. Can be URLs or arbitrary text.
localhost, tiktok.com

Use New Scraper
Use experimental new scraper, seems to work well on desktop but not mobile.

Enhance Default Paste and *Enhance Drop Events* will make a request to the URL you are pasting and fetch the HTML title. This title is then used to rename the link using markdown syntax "`[]()`".

7.2.2 Footnote Shortcut

These are my settings:



Footnote Shortcut

Need help? Check the README!

Enable Footnote Autosuggest
Suggests existing footnotes when entering named footnotes.

Footnotes Section Behavior

Enable Footnote Section Heading
Automatically adds a heading separating footnotes at the bottom of the note from the rest of the text.

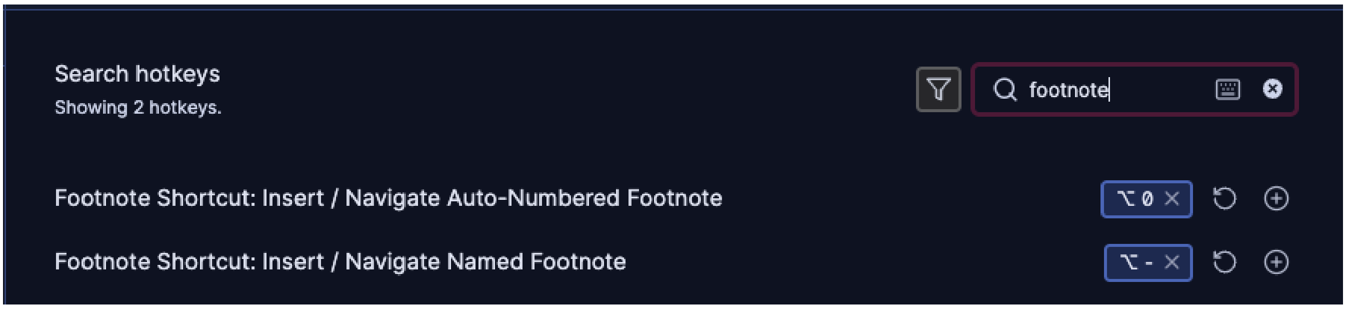
Footnote Section Heading
Heading to place above footnotes section (Supports Markdown formatting). Heading will be H1 size.
References

I turned *Enable Footnote Section Heading* on, this will create a new section at the bottom of your note containing all your footnotes. This is optional but I personally like being able to see and click my "References" section at the bottom of my note outline.

You can use whatever name you like for the *Footnote Section Heading* option.

7.2.2.1 Footnote Hotkeys

Before moving on, you should customize hotkeys for using this plugin. Open up the Settings Window and go to Options > Hotkeys; write "footnote" on the search bar.



Footnote Shortcut: Insert / Navigate Auto-Numbered Footnote ⌥ 0

Footnote Shortcut: Insert / Navigate Named Footnote ⌥ -

In my case I have `Alt + 0` to insert an auto-numbered footnote and `Alt + -` to insert a named footnote.

After setting this plugin up, try using the shortcut in a new note.

Write a sentence and try inserting an auto-numbered footnote with `Alt + 0`. Doing this will create a footnote link in your sentence and automatically place your cursor on the automatically created footnote section. Enter the URL link there, Auto Link Title will take care of the URL name and by hitting Alt + 0, you will be taken back to the original text.

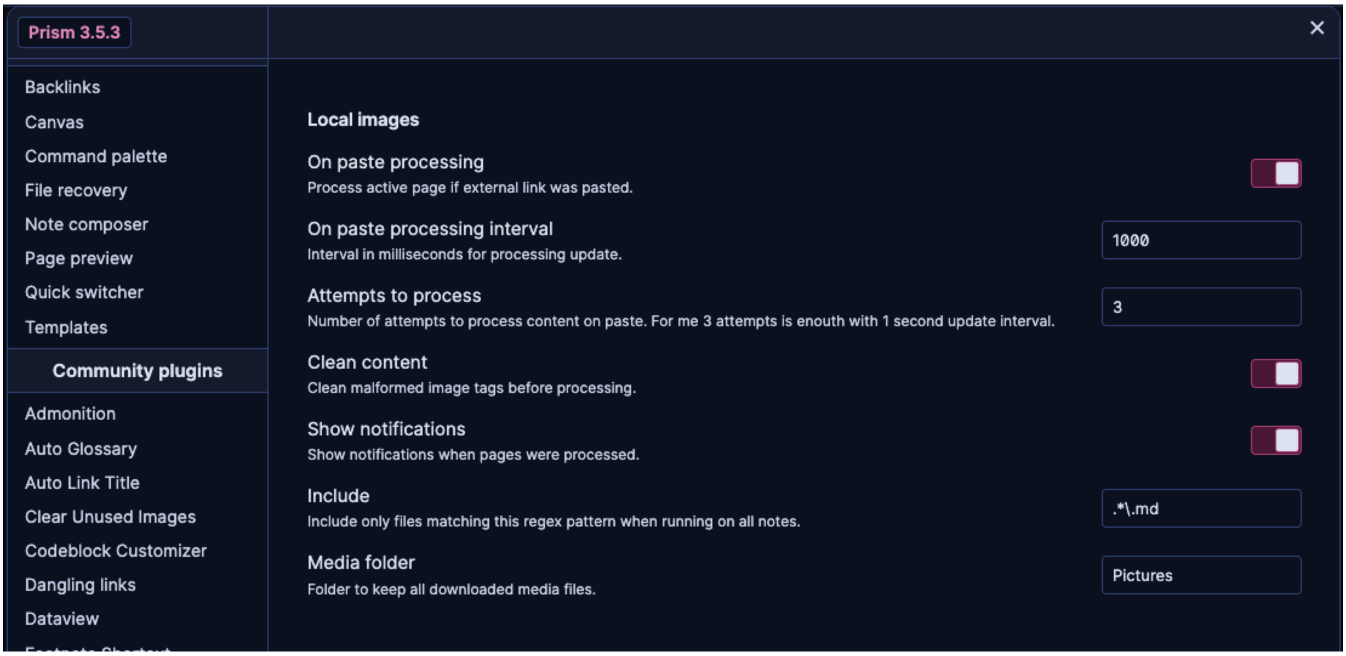
> This methodology is a huge time saver since you don't have to worry about creating the footnote link using `[^1]` scrolling down to the bottom, creating a new section, creating the actual footnote and scrolling back.

7.2.3 Linter

Because this plugin is designed to format your notes according to your preferred style settings, I suggest configuring it to match your personal preferences. This setup should take about 5 minutes and will yield results tailored to your liking. However, if you prefer, you can use my personal settings. To do so, open the settings window, navigate to *Community Plugins*, and select *Linter*.

7.2.4 Local Images

Here are my settings:



Local images

On paste processing
Process active page if external link was pasted.

On paste processing interval: 1000
Interval in milliseconds for processing update.

Attempts to process: 3
Number of attempts to process content on paste. For me 3 attempts is enouth with 1 second update interval.

Clean content
Clean malformed image tags before processing.

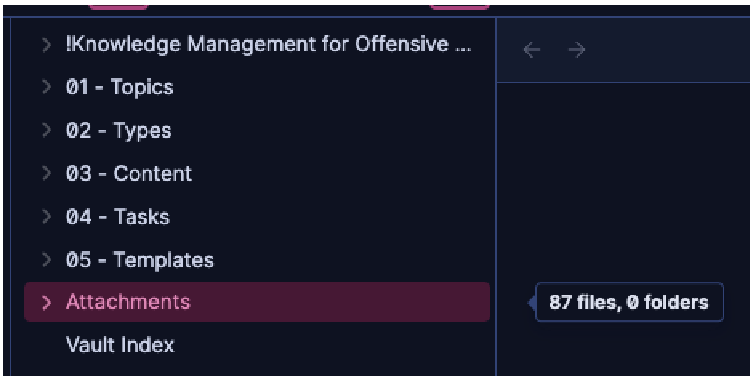
Show notifications
Show notifications when pages were processed.

Include: .*\.md
Include only files matching this regex pattern when running on all notes.

Media folder: Pictures
Folder to keep all downloaded media files.

I have the *On Paste Processing* setting enabled because I want this plugin to work automatically whenever I paste an image from the Internet.

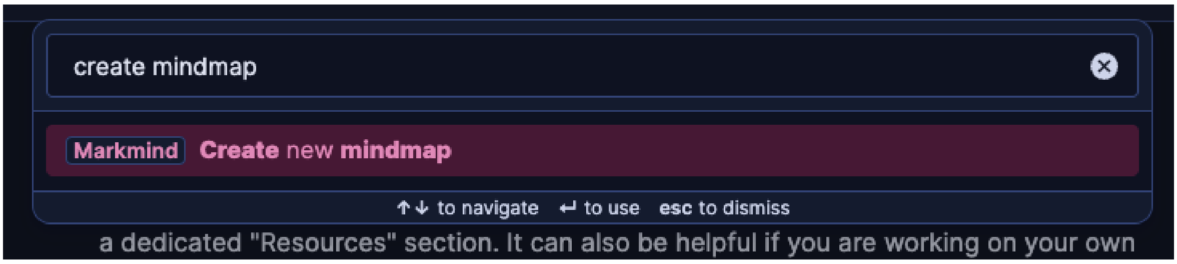
Set the *Media Folder* to your desired attachments folder. For this course, we are using "Attachments," as explained in [2. Getting to Know the Vault](). Any image URL will automatically download the image and save it to that folder.



7.2.5 Markmind

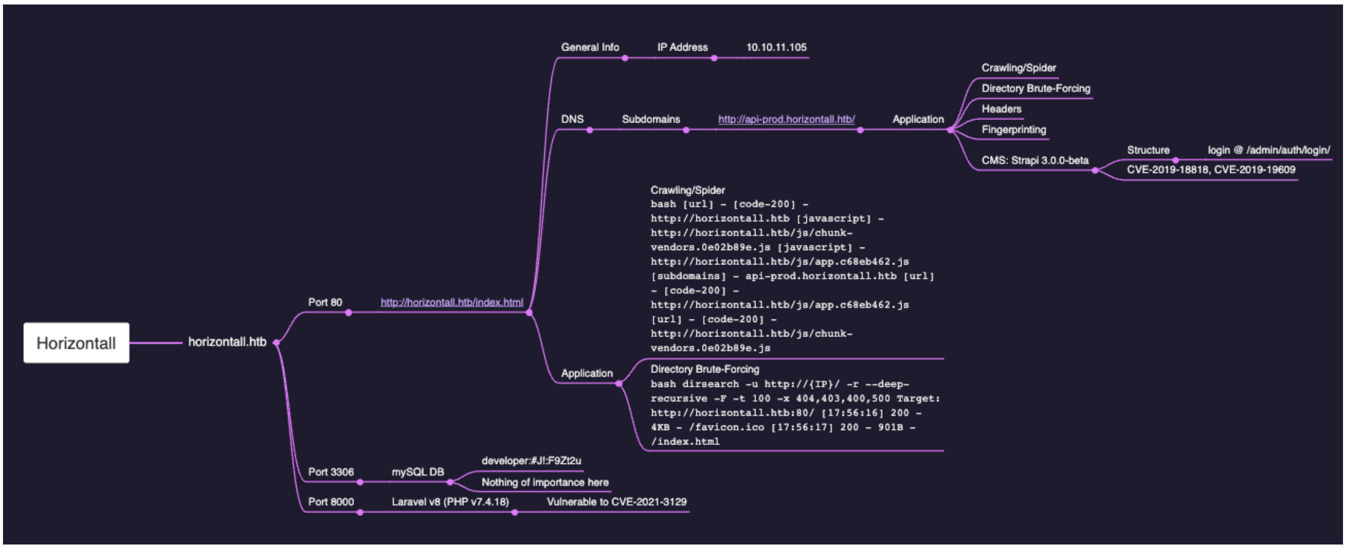
I have not customized the settings for this plugin and don't use it much nowadays. I prefer using Obsidian's built-in canvas feature because it is more intuitive. However, I know that several people prefer using mindmaps for their methodology, which is why I included it here.

Once installed, you can create a mindmap by opening the command palette (Cmd + P or Ctrl + P) and selecting the *Create New Mindmap* option.


create mindmap
Markmind Create new mindmap
↑↓ to navigate ↵ to use esc to dismiss
a dedicated "Resources" section. It can also be helpful if you are working on your own

I suggest reading the official documentation for more detailed instructions, as the plugin offers many options and can become quite complex. Again, in my opinion, Obsidian's canvas is a superior option, and I will demonstrate how I use it in my daily workflow in a subsequent section.

The following picture is an example from a long time ago when I was experimenting using mindmaps for tracking my progress on my first Hack the Box machines.

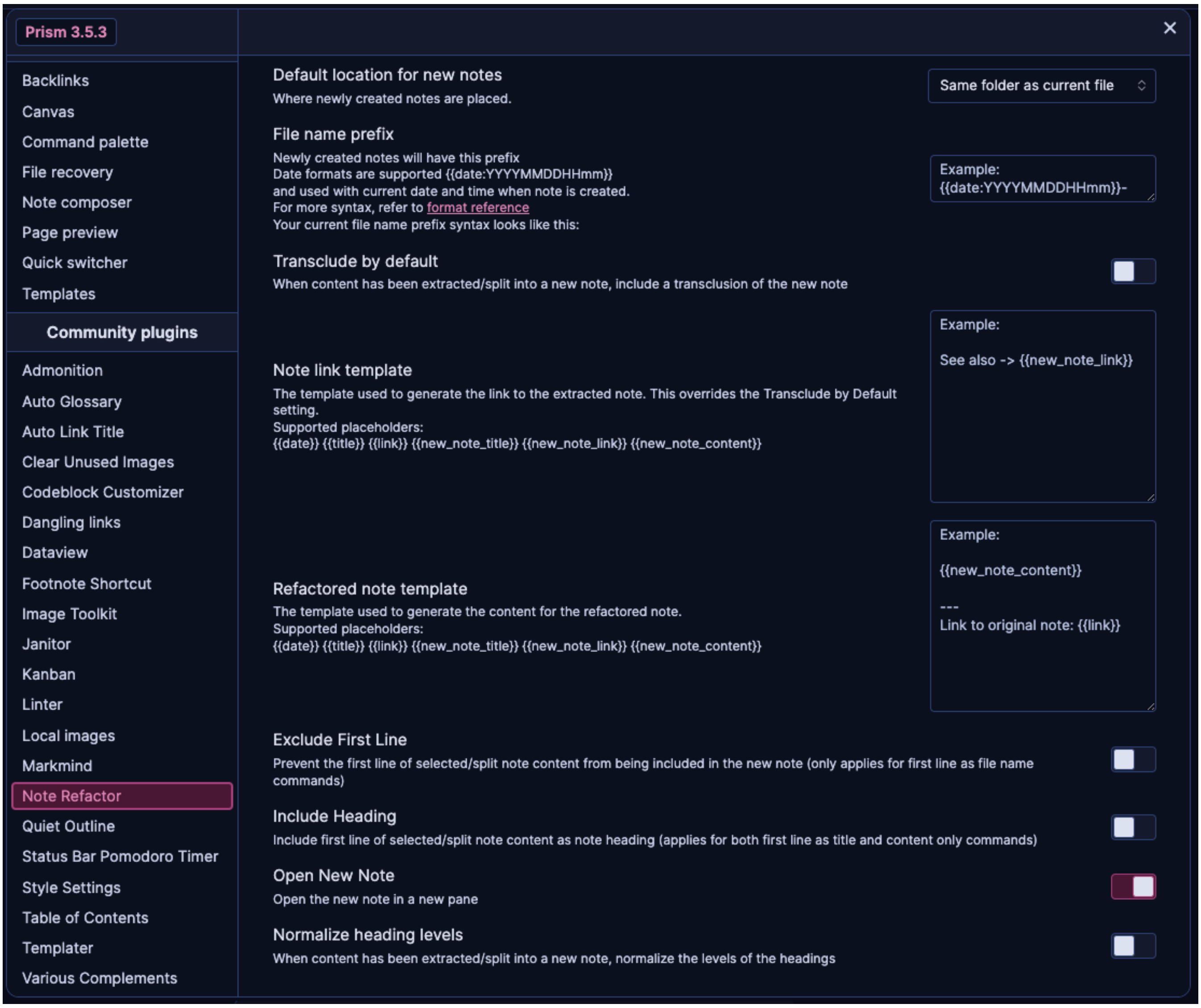


```
bash [url] - [code-200] -
http://horizontall.htb [javascript] -
http://horizontall.htb/js/chunk-
vendors.0e02b89e.js [javascript] -
http://horizontall.htb/js/app.c68eb462.js
[subdomains] - api-prod.horizontall.htb [url]
- [code-200] -
http://horizontall.htb/js/app.c68eb462.js
[url] - [code-200] -
http://horizontall.htb/js/chunk-
vendors.0e02b89e.js
```

```
bash dirsearch -u http://{IP}/ -r --deep-
recursive -F -t 100 -x 404,403,400,500 Target:
http://horizontall.htb:80/ [17:56:16] 200 -
4KB - /favicon.ico [17:56:17] 200 - 901B -
/index.html
```

7.2.6 Note Refactor

These are my settings:



Default location for new notes
Where newly created notes are placed.
Same folder as current file

File name prefix
Newly created notes will have this prefix
Date formats are supported {{date:YYYYMMDDHHmm}}
and used with current date and time when note is created.
For more syntax, refer to format reference
Your current file name prefix syntax looks like this:
Example:
{{date:YYYYMMDDHHmm}}-

Transclude by default ☐
When content has been extracted/split into a new note, include a transclusion of the new note

Note link template
The template used to generate the link to the extracted note. This overrides the Transclude by Default setting.
Supported placeholders:
{{date}} {{title}} {{link}} {{new_note_title}} {{new_note_link}} {{new_note_content}}
Example:

See also -> {{new_note_link}}

Refactored note template
The template used to generate the content for the refactored note.
Supported placeholders:
{{date}} {{title}} {{link}} {{new_note_title}} {{new_note_link}} {{new_note_content}}
Example:

{{new_note_content}}

Link to original note: {{link}}

Exclude First Line ☐
Prevent the first line of selected/split note content from being included in the new note (only applies for first line as file name commands)

Include Heading ☐
Include first line of selected/split note content as note heading (applies for both first line as title and content only commands)

Open New Note ☑
Open the new note in a new pane

Normalize heading levels ☐
When content has been extracted/split into a new note, normalize the levels of the headings

This plugin is particularly useful for splitting monolithic or very long notes into multiple single-concept linked notes.

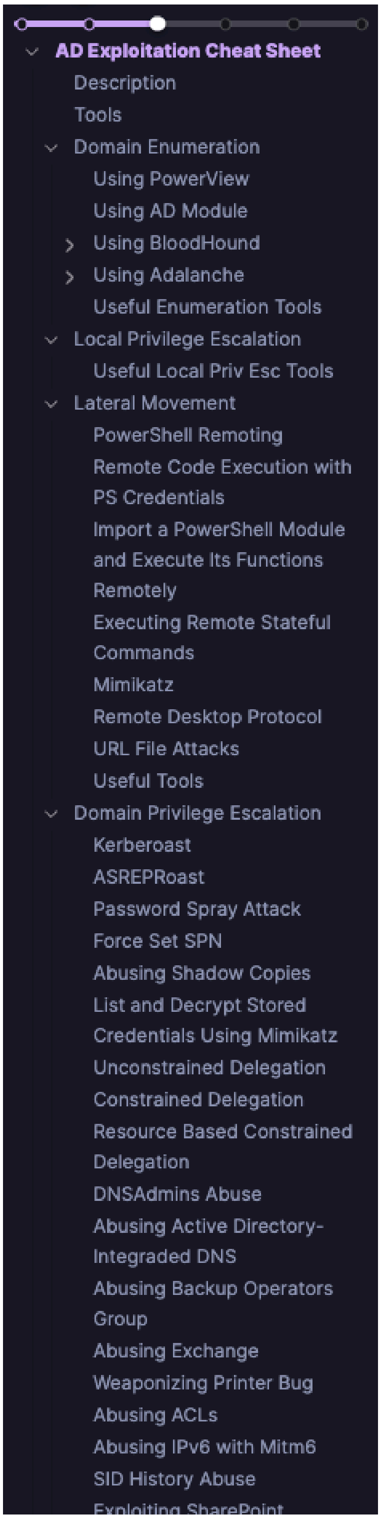
7.2.6.1 Refactoring a Monolithic Note Example

Some time ago, when I was experimenting with my note-taking methodology, I created a very long cheatsheet note compiling commands needed for pentesting an Active Directory environment. This note was extremely difficult to navigate, and I often forgot which concepts were included.

In this section, I will teach you how I would tackle splitting massive notes into modular notes.

> The cheatsheets used in this example comes from S1ckB0y1337's Active Directory cheatsheet.
> You can review the example notes I made for this section: Active Directory Penetration Testing Methodology Cheatsheet ADPT Discovery

Here is a picture of the note's outline (it continues further down):



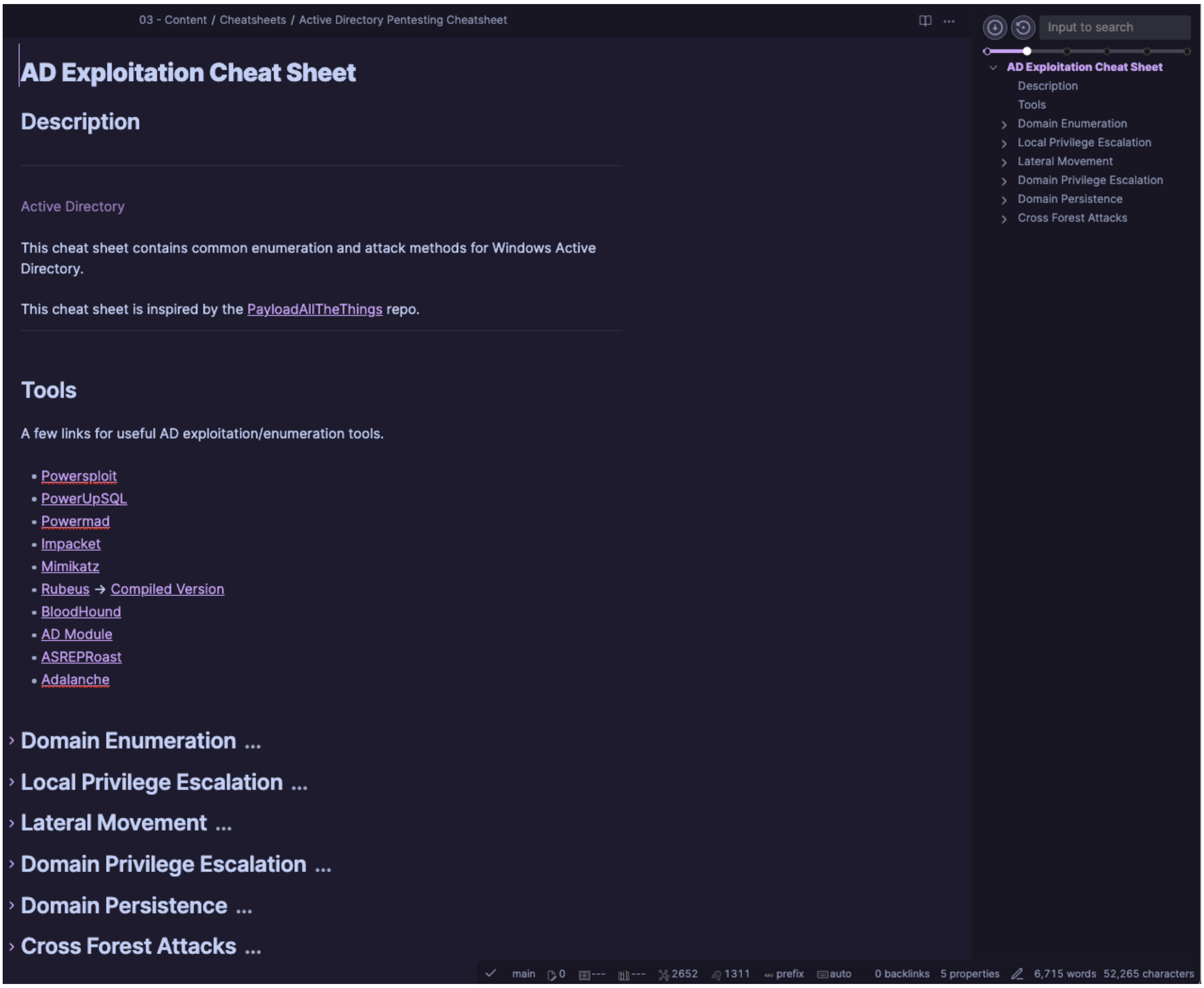
- AD Exploitation Cheat Sheet
  - Description
  - Tools
  - Domain Enumeration
    - Using PowerView
    - Using AD Module
    - Using BloodHound
    - Using Adalanche
    - Useful Enumeration Tools
  - Local Privilege Escalation
    - Useful Local Priv Esc Tools
  - Lateral Movement
    - PowerShell Remoting
    - Remote Code Execution with PS Credentials
    - Import a PowerShell Module and Execute Its Functions Remotely
    - Executing Remote Stateful Commands
    - Mimikatz
    - Remote Desktop Protocol
    - URL File Attacks
    - Useful Tools
  - Domain Privilege Escalation
    - Kerberoast
    - ASREPRoast
    - Password Spray Attack
    - Force Set SPN
    - Abusing Shadow Copies
    - List and Decrypt Stored Credentials Using Mimikatz
    - Unconstrained Delegation
    - Constrained Delegation
    - Resource Based Constrained Delegation
    - DNSAdmins Abuse
    - Abusing Active Directory-Integraded DNS
    - Abusing Backup Operators Group
    - Abusing Exchange
    - Weaponizing Printer Bug
    - Abusing ACLs
    - Abusing IPv6 with Mitm6
    - SID History Abuse
    - Exploiting SharePoint

Clearly, this way of taking notes is inefficient and does not foster collaboration. Imagine having to sift through a note like this from a colleague to find information.

You might already have a note that looks similar. You will now learn how to convert it into a more usable format.

7.2.6.2 Reviewing the Note

Start by identifying the various concepts discussed in the note.


03 - Content / Cheatsheets / Active Directory Pentesting Cheatsheet
Input to search
AD Exploitation Cheat Sheet
Description
Tools
Domain Enumeration
Local Privilege Escalation
Lateral Movement
Domain Privilege Escalation
Domain Persistence
Cross Forest Attacks
main 0 --- --- 2652 1311 prefix auto 0 backlinks 5 properties 6,715 words 52,265 characters

AD Exploitation Cheat Sheet

Description

Active Directory

This cheat sheet contains common enumeration and attack methods for Windows Active Directory.

This cheat sheet is inspired by the PayloadAllTheThings repo.

Tools

A few links for useful AD exploitation/enumeration tools.

- Powersploit
- PowerUpSQL
- Powermad
- Impacket
- Mimikatz
- Rubeus → Compiled Version
- BloodHound
- AD Module
- ASREPRoast
- Adalanche

Domain Enumeration ...

Local Privilege Escalation ...

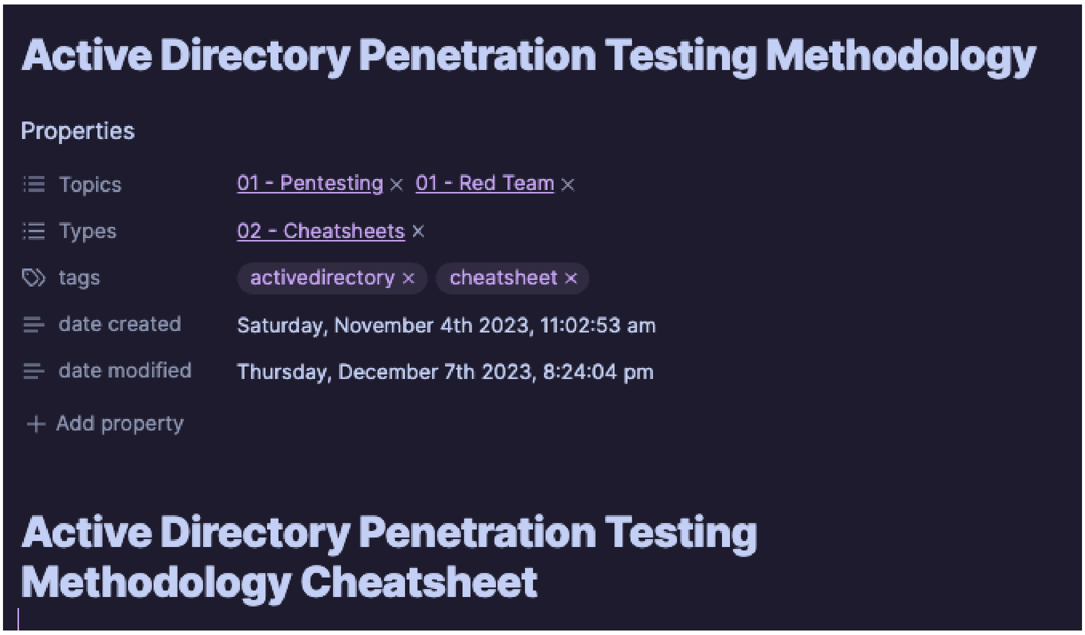
Lateral Movement ...

Domain Privilege Escalation ...

Domain Persistence ...

Cross Forest Attacks ...

First, we could use a more accurate title. Since we are performing more than just exploitation, we could rename the note to *Active Directory Penetration Testing Methodology Cheatsheet*.



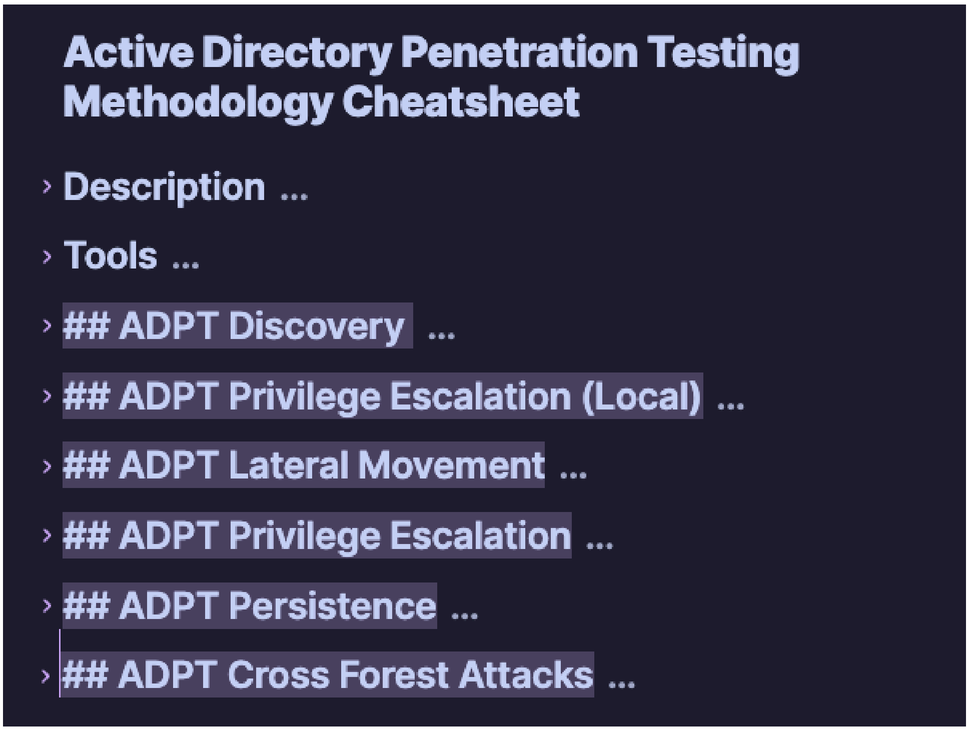
Active Directory Penetration Testing Methodology

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Types	02 - Cheatsheets ×
tags	activedirectory × cheatsheet ×
date created	Saturday, November 4th 2023, 11:02:53 am
date modified	Thursday, December 7th 2023, 8:24:04 pm

Active Directory Penetration Testing Methodology Cheatsheet

The note's section titles are not as precise as they could be. Since the original note will serve as a wrapper containing the other notes, I will use a prefix (ADPT) to identify the other notes as children of this one.



Active Directory Penetration Testing Methodology Cheatsheet

› Description ...

› Tools ...

› ## ADPT Discovery ...

› ## ADPT Privilege Escalation (Local) ...

› ## ADPT Lateral Movement ...

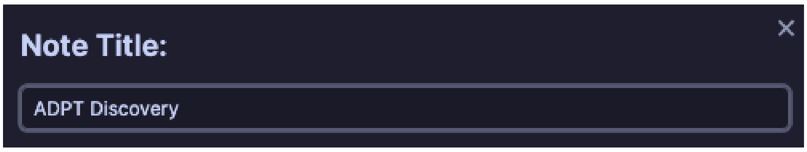
› ## ADPT Privilege Escalation ...

› ## ADPT Persistence ...

› ## ADPT Cross Forest Attacks ...

7.2.6.3 Refactoring the Note

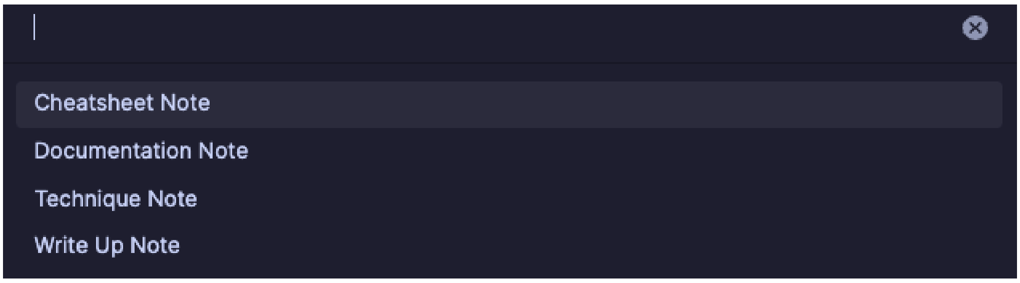
Now copy and paste the title of the first heading, "ADPT Discovery," and hit Cmd + N or Ctrl + N to create a new note. Paste the title into the Note Title prompt.



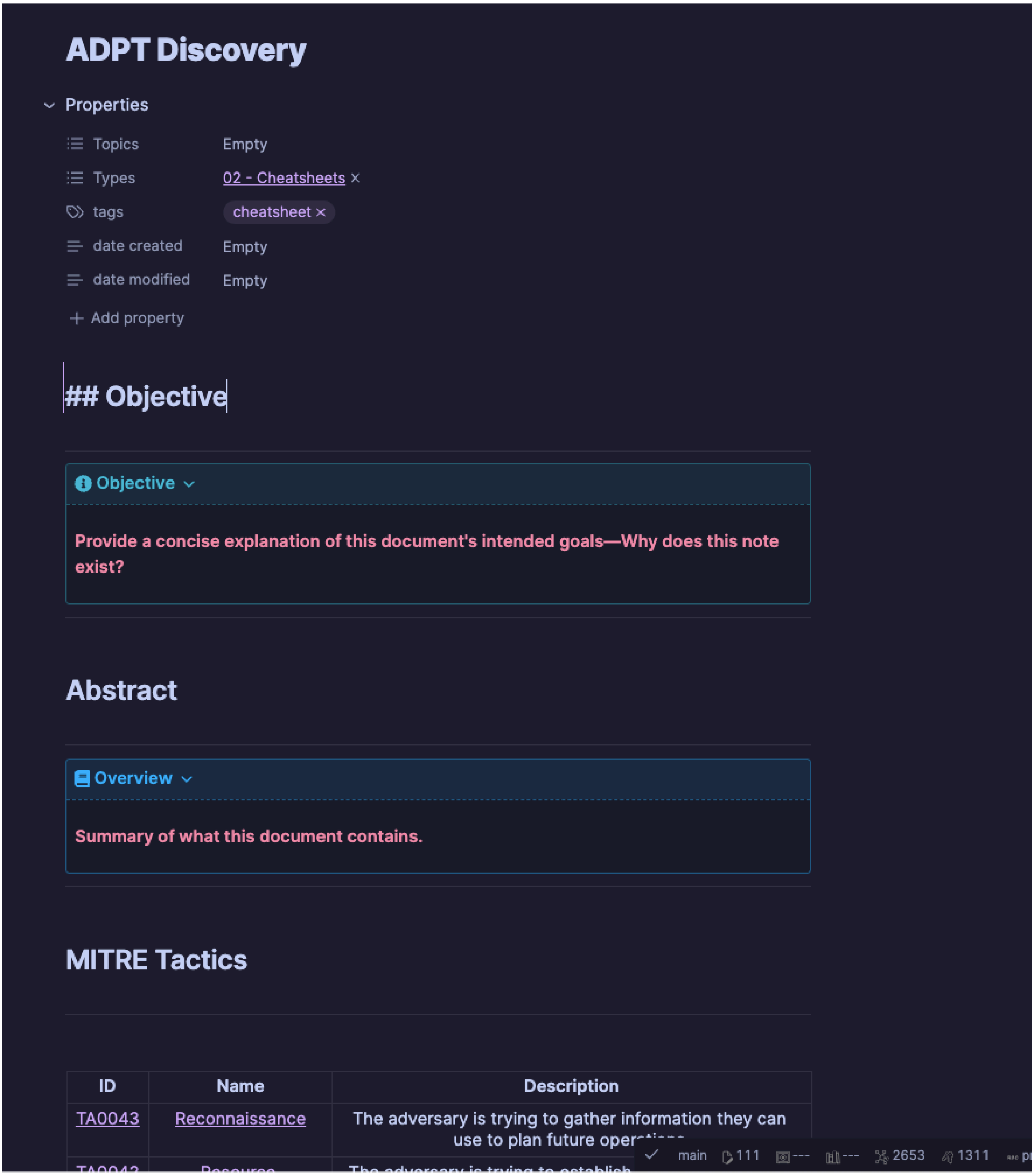
Note Title:

ADPT Discovery

Select "Cheatsheet" note from the Note Type prompt.



Now we have a note dedicated to "Discovery".



ADPT Discovery

Properties

Topics	Empty
Types	02 - Cheatsheets ×
tags	cheatsheet ×
date created	Empty
date modified	Empty

+ Add property

Objective

Objective

Provide a concise explanation of this document's intended goals—Why does this note exist?

Abstract

Overview

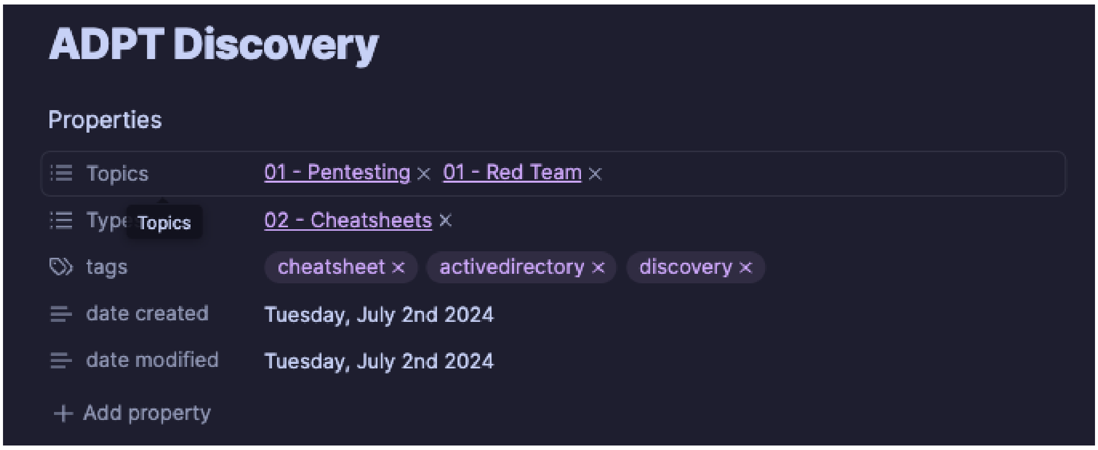
Summary of what this document contains.

MITRE Tactics

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future oper
TA0042	Resource	The adversary is trying to establish

Fill in the metadata before proceeding with the note:

- Feel free to use the same *Note Types* from the parent note (Pentesting and Red Team).
- Proceed to lint the file using your hotkey (mine is `Cmd + Alt + L`) or the command palette (`Cmd + P` or `Ctrl + P`), and choose "Lint the current file." This will take care of the date and any style inconsistencies.
- Add the corresponding tags. In this case, I am using "activedirectory" and "discovery."



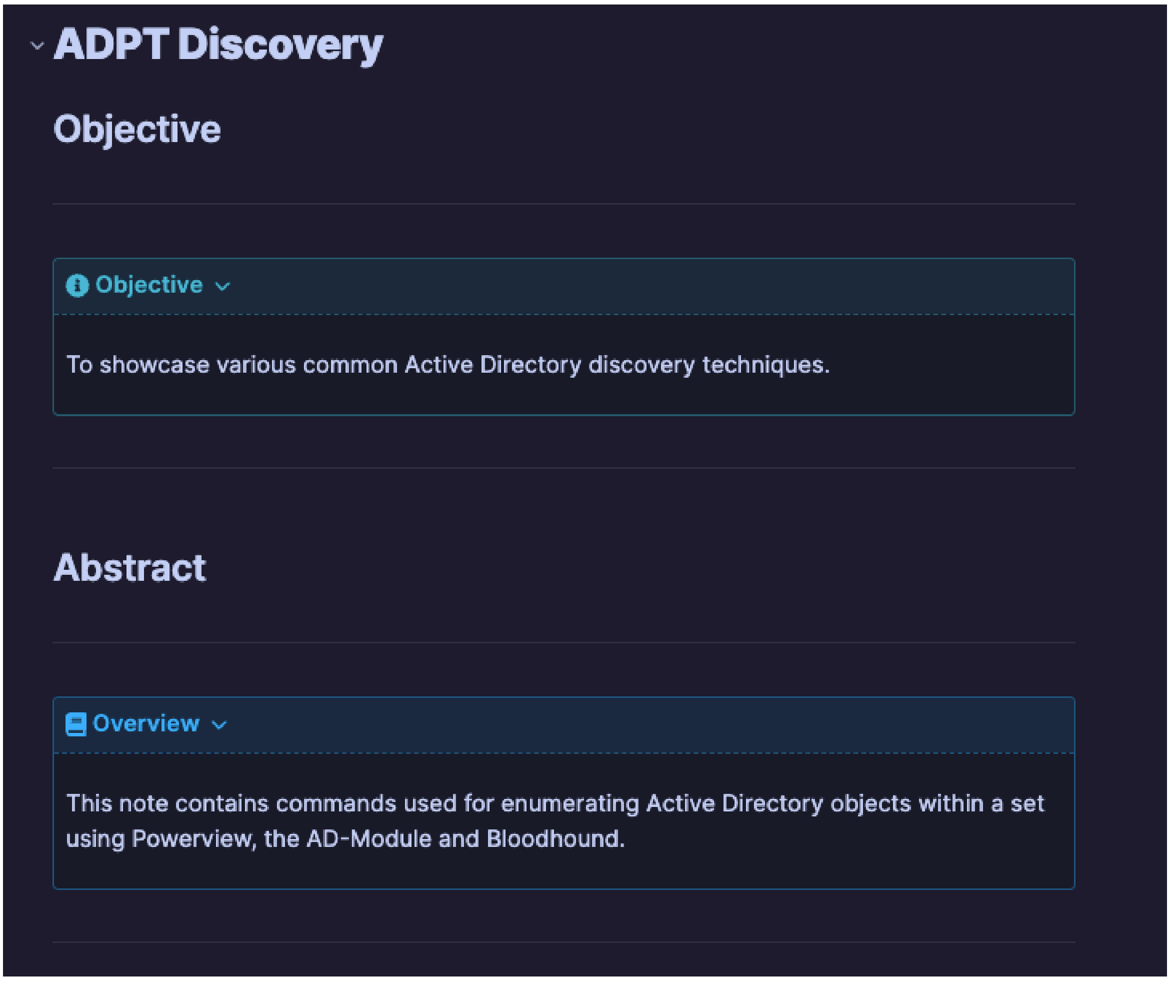
ADPT Discovery

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Type	02 - Cheatsheets ×
tags	cheatsheet × activedirectory × discovery ×
date created	Tuesday, July 2nd 2024
date modified	Tuesday, July 2nd 2024

> Note that the word "Discovery" comes from the MITRE ATT&CK Matrix for Enterprise, which categorizes hacking techniques used in Penetration Tests and Red Team engagements. It is common for hacking certifications and training programs to use the word "Enumeration" instead of "Discovery." They also commonly mix "Lateral Movement" techniques with "Credential Access" techniques. I like to keep my notes as accurate as possible and use this Matrix as my compass.

Then proceed by filling in the Objective and Abstract callouts with simple descriptions so anyone glancing over this note in the future (including yourself) can understand what it contains without wasting too much time.



ADPT Discovery

Objective

Objective

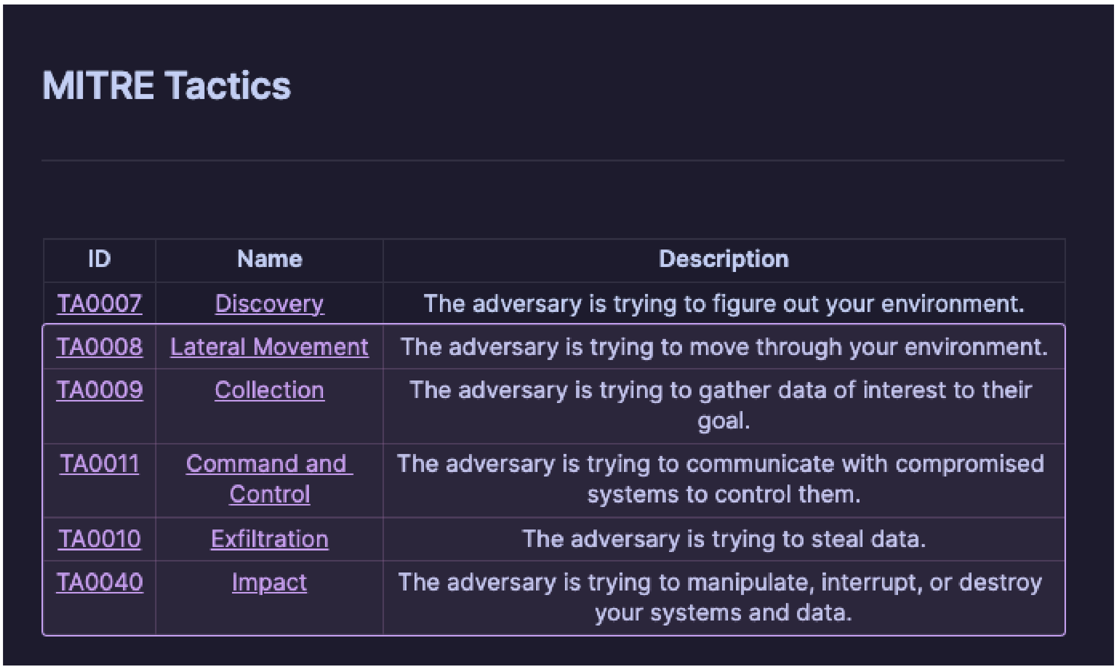
To showcase various common Active Directory discovery techniques.

Abstract

Overview

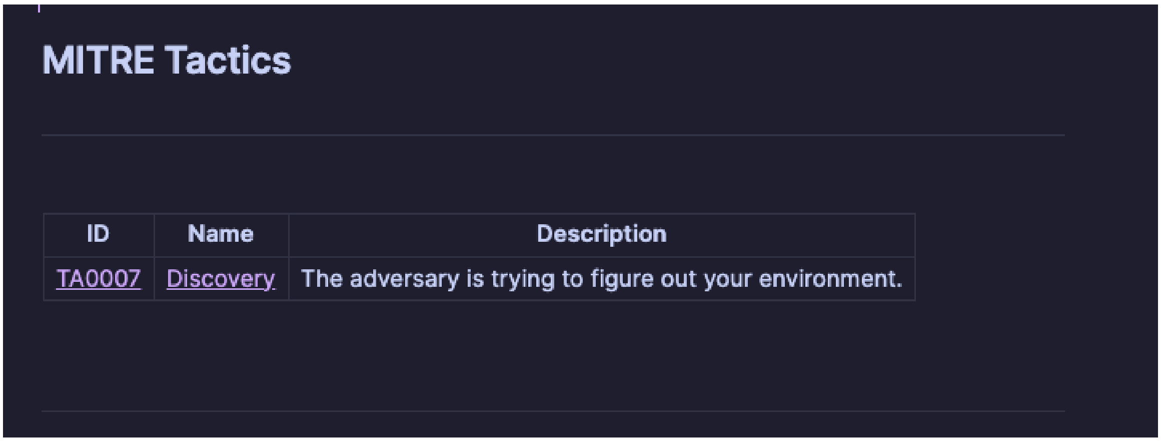
This note contains commands used for enumerating Active Directory objects within a set using Powerview, the AD-Module and Bloodhound.

Proceed to the "MITRE Tactics" section and remove any techniques that are not relevant to the topic at hand. In this case, we are only keeping "Discovery." You can remove multiple rows using your mouse by clicking and dragging or using your keyboard's Shift and arrow keys.



MITRE Tactics

ID	Name	Description
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

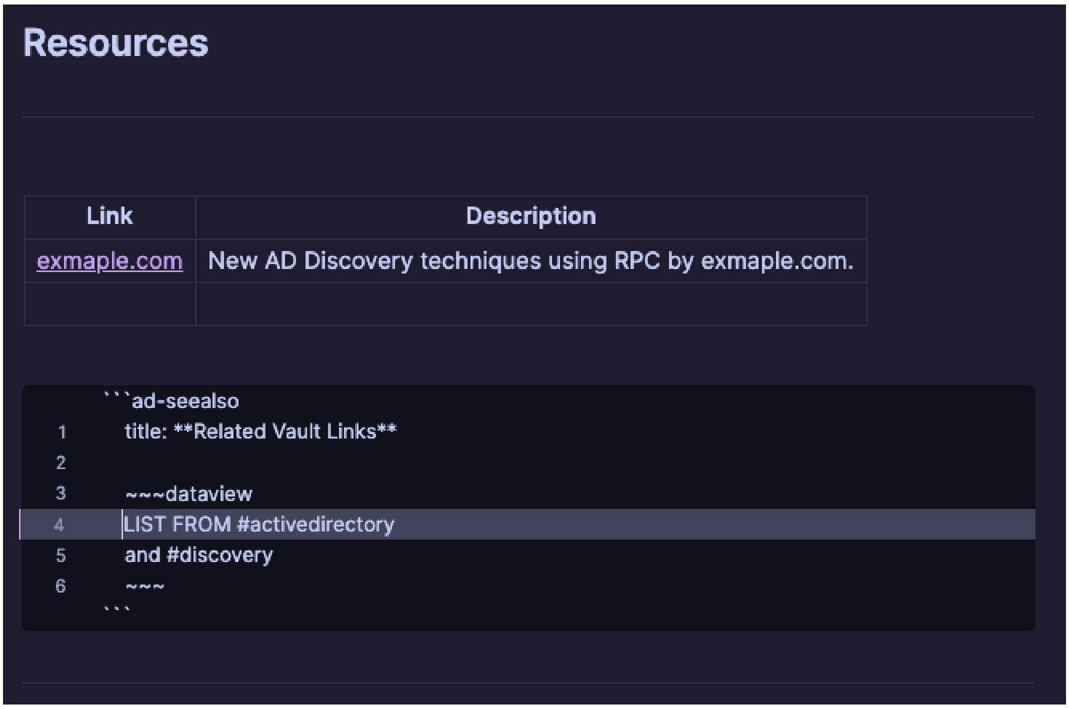


MITRE Tactics

ID	Name	Description
TA0007	Discovery	The adversary is trying to figure out your environment.

At this point, I would fill in the "Resources" section.

- This is optional, but you could create an admonition list using all notes related to "Active Directory" and "Discovery."
- In the future, if I stumble upon a blog post containing new discovery techniques, I could add it to the resources table with a short description.



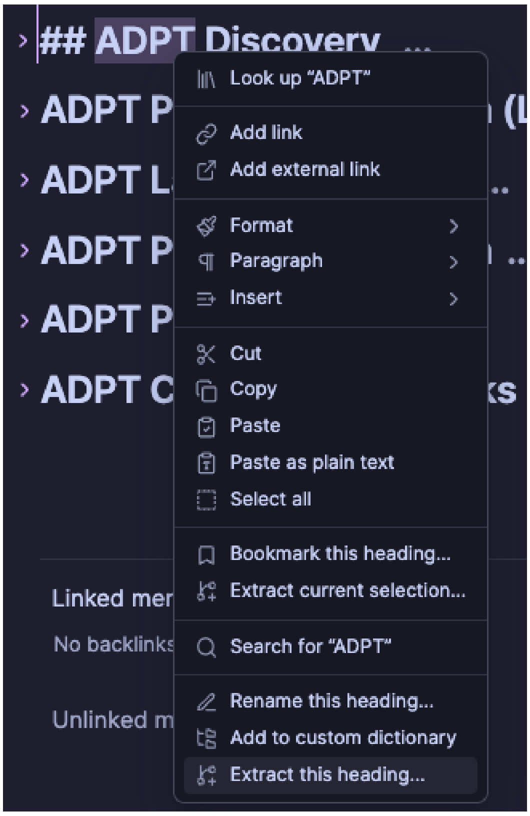
Resources

Link	Description
exmaple.com	New AD Discovery techniques using RPC by exmaple.com.

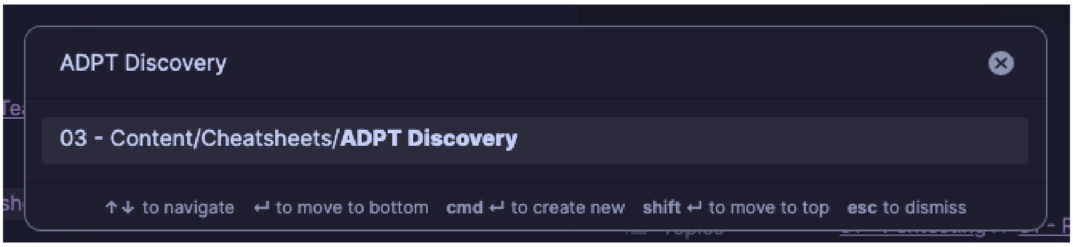
````
```ad-seealso
title: **Related Vault Links**

~~~dataview
LIST FROM #activedirectory
and #discovery
~~~
```
````

Now I will go to the parent note and right-click the "ADPT Discovery" heading.

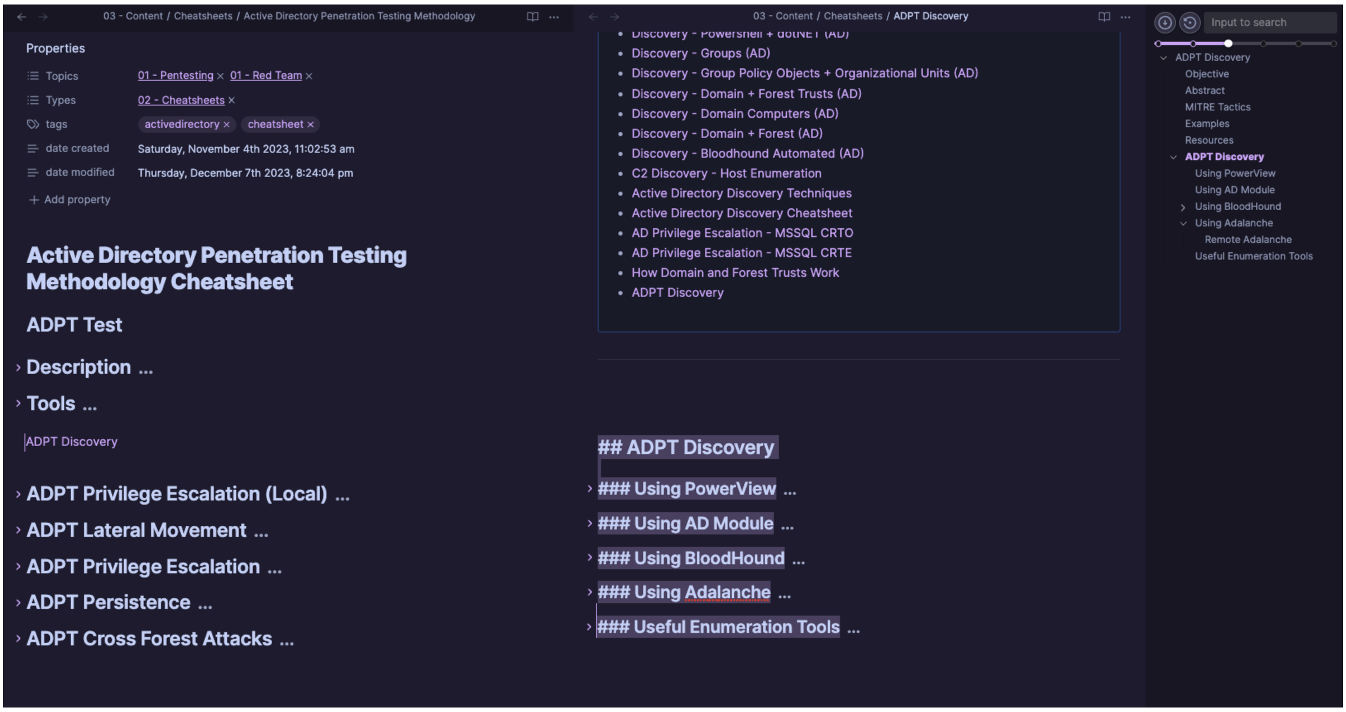
The last option shown in the menu is from the Note Refactor plugin and allows you to extract the heading and move it to a new existing note (If there is no existing note, it will create one for you with that name).



After clicking "Extract this heading...", you will see a prompt asking which note to append this heading to. Since I already have a note with the same name as the heading, the program detects it and lets me choose it.



As you can see, the heading disappears from the parent note (Active Directory Penetration Testing Methodology Cheatsheet), leaving us with a link to the child note (ADPT Discovery). The original heading `## ADPT Discovery` is then appended to the child note.



03 - Content / Cheatsheets / Active Directory Penetration Testing Methodology

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Types	02 - Cheatsheets ×
tags	activedirectory × cheatsheet ×
date created	Saturday, November 4th 2023, 11:02:53 am
date modified	Thursday, December 7th 2023, 8:24:04 pm

+ Add property

Active Directory Penetration Testing Methodology Cheatsheet

ADPT Test

› Description ...

› Tools ...

ADPT Discovery

› ADPT Privilege Escalation (Local) ...

› ADPT Lateral Movement ...

› ADPT Privilege Escalation ...

› ADPT Persistence ...

› ADPT Cross Forest Attacks ...

03 - Content / Cheatsheets / ADPT Discovery

- Discovery - Powershell + dotNET (AD)
- Discovery - Groups (AD)
- Discovery - Group Policy Objects + Organizational Units (AD)
- Discovery - Domain + Forest Trusts (AD)
- Discovery - Domain Computers (AD)
- Discovery - Domain + Forest (AD)
- Discovery - Bloodhound Automated (AD)
- C2 Discovery - Host Enumeration
- Active Directory Discovery Techniques
- Active Directory Discovery Cheatsheet
- AD Privilege Escalation - MSSQL CRTO
- AD Privilege Escalation - MSSQL CRTE
- How Domain and Forest Trusts Work
- ADPT Discovery

ADPT Discovery

› ### Using PowerView ...

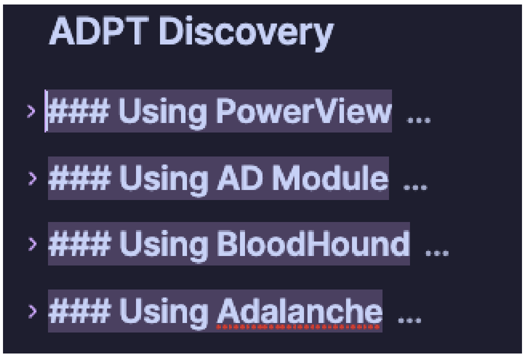
› ### Using AD Module ...

› ### Using BloodHound ...

› ### Using Adalanche ...

› ### Useful Enumeration Tools ...

Now we can fill the "Examples" section of the child note using the "ADPT Discovery" heading's subsections.



ADPT Discovery

› ### Using PowerView ...

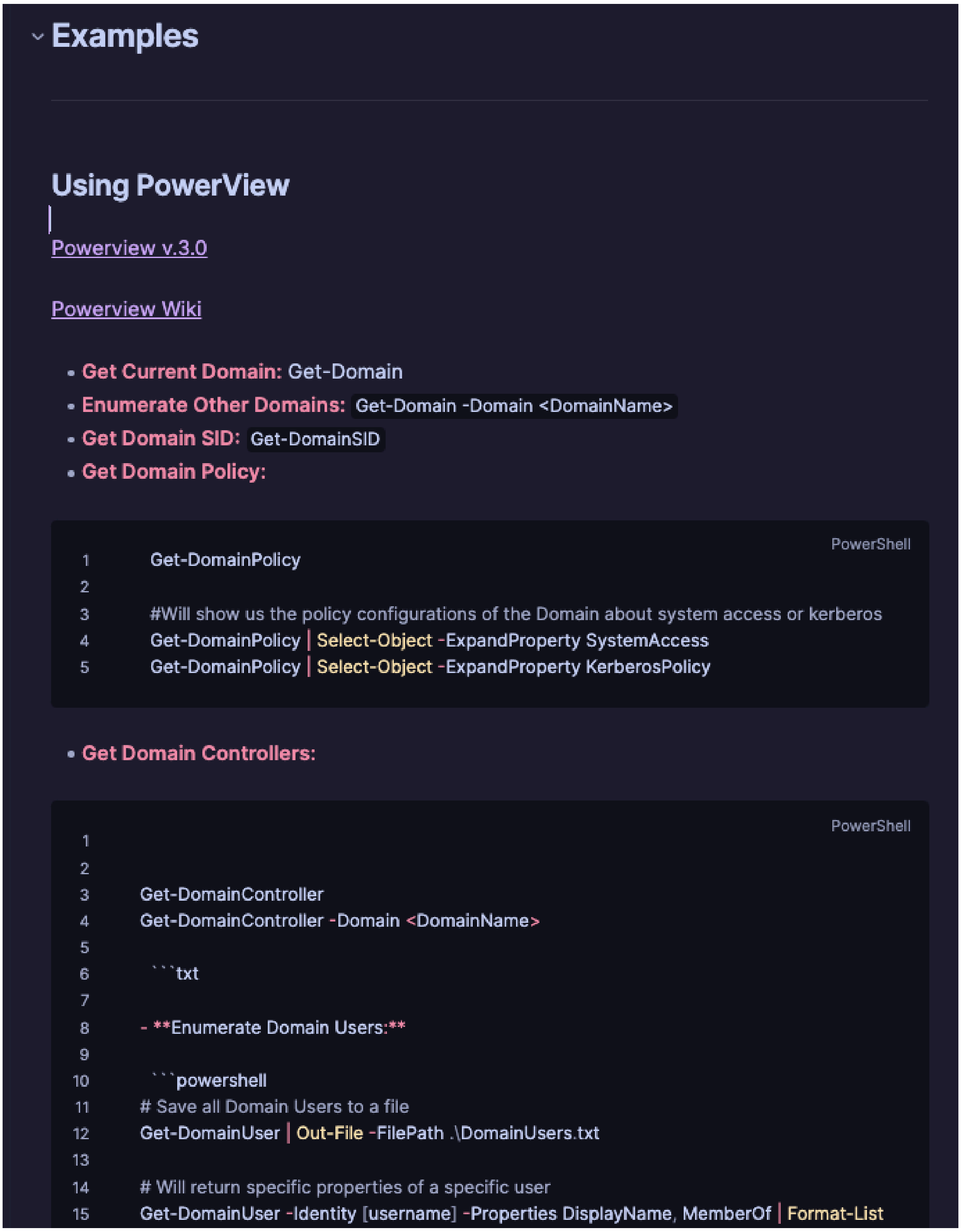
› ### Using AD Module ...

› ### Using BloodHound ...

› ### Using Adalanche ...

**

You can cut and paste these level 3 headings into the "Examples" section.



Examples

Using PowerView

Powerview v.3.0

Powerview Wiki

- **Get Current Domain:** Get-Domain
- **Enumerate Other Domains:** `Get-Domain -Domain <DomainName>`
- **Get Domain SID:** `Get-DomainSID`
- **Get Domain Policy:**

````
PowerShell
    Get-DomainPolicy

    #Will show us the policy configurations of the Domain about system access or kerberos
    Get-DomainPolicy | Select-Object -ExpandProperty SystemAccess
    Get-DomainPolicy | Select-Object -ExpandProperty KerberosPolicy
````

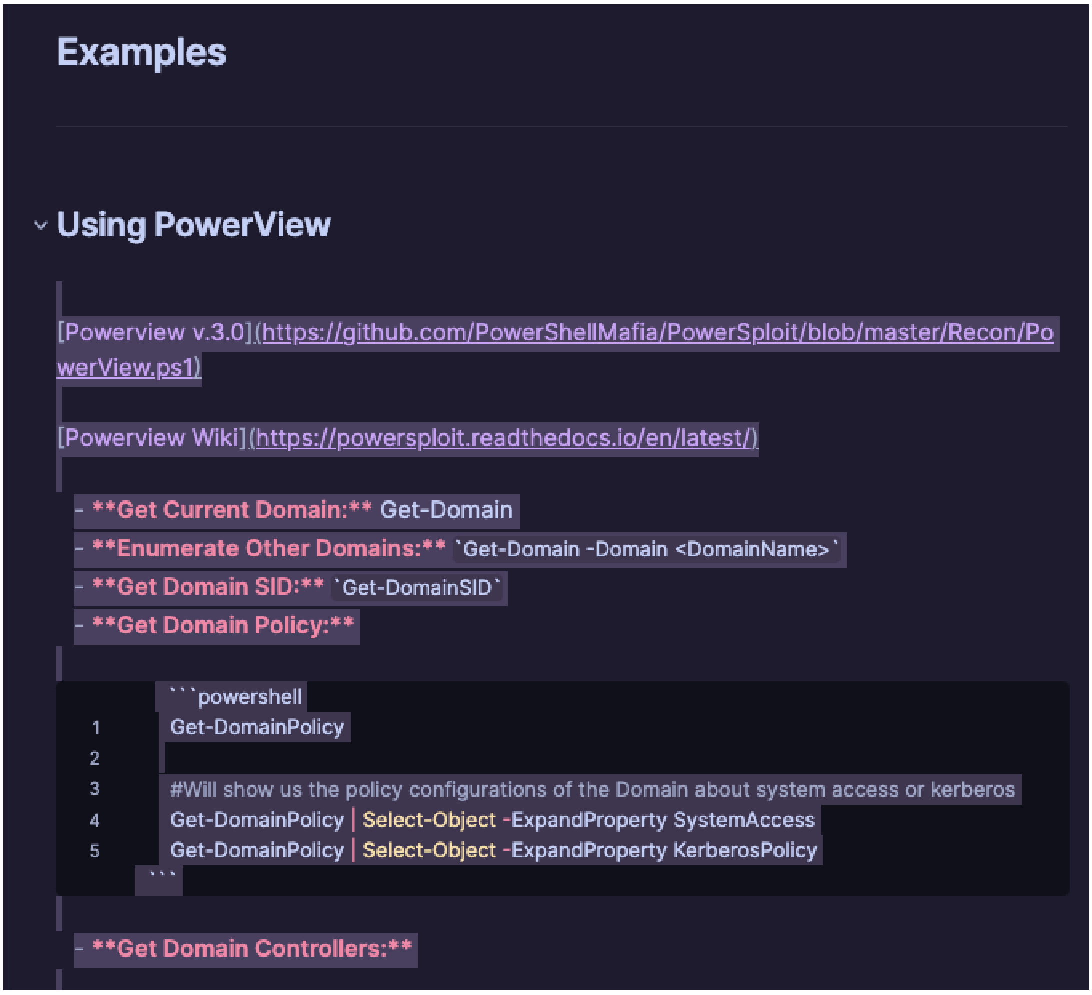
- **Get Domain Controllers:**

~~~
PowerShell


Get-DomainController
Get-DomainController -Domain <DomainName>

  ```txt

- **Enumerate Domain Users:**

  ```powershell
# Save all Domain Users to a file
Get-DomainUser | Out-File -FilePath .\DomainUsers.txt

# Will return specific properties of a specific user
Get-DomainUser -Identity [username] -Properties DisplayName, MemberOf | Format-List
~~~

At this point, you could select the whole subsection's contents and create a new "ad-example" type admonition callout to contain it. You can set a hotkey for *Insert Admonition* by going to the Settings window under Hotkeys. I use `Cmd + Shift + A` or `Ctrl + Shift + A`.

In this case, I won't be using the *Insert Admonition* command because it uses three backticks to create the block, and this section contains various triple backtick code blocks. This is a common issue, and to solve it, we can leverage triple wave dashes `~` or more than three backticks.

Select the whole section, leaving a blank newline both above and below.



Examples

Using PowerView

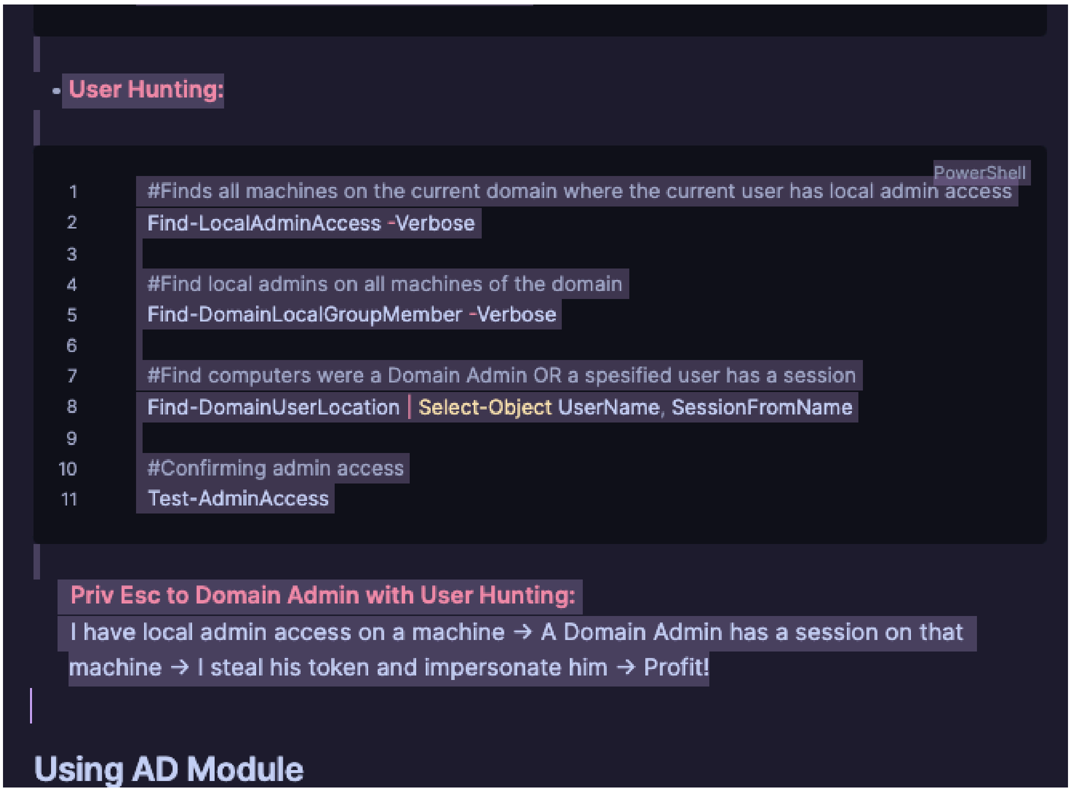
~~~~
[Powerview v.3.0](https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1)

[Powerview Wiki](https://powersploit.readthedocs.io/en/latest/)

- **Get Current Domain:** Get-Domain
- **Enumerate Other Domains:** `Get-Domain -Domain <DomainName>`
- **Get Domain SID:** `Get-DomainSID`
- **Get Domain Policy:**

    ```powershell
    Get-DomainPolicy

    #Will show us the policy configurations of the Domain about system access or kerberos
    Get-DomainPolicy | Select-Object -ExpandProperty SystemAccess
    Get-DomainPolicy | Select-Object -ExpandProperty KerberosPolicy
  ```

- **Get Domain Controllers:**
~~~~



- User Hunting:

PowerShell

```powershell
#Finds all machines on the current domain where the current user has local admin access
Find-LocalAdminAccess -Verbose

#Find local admins on all machines of the domain
Find-DomainLocalGroupMember -Verbose

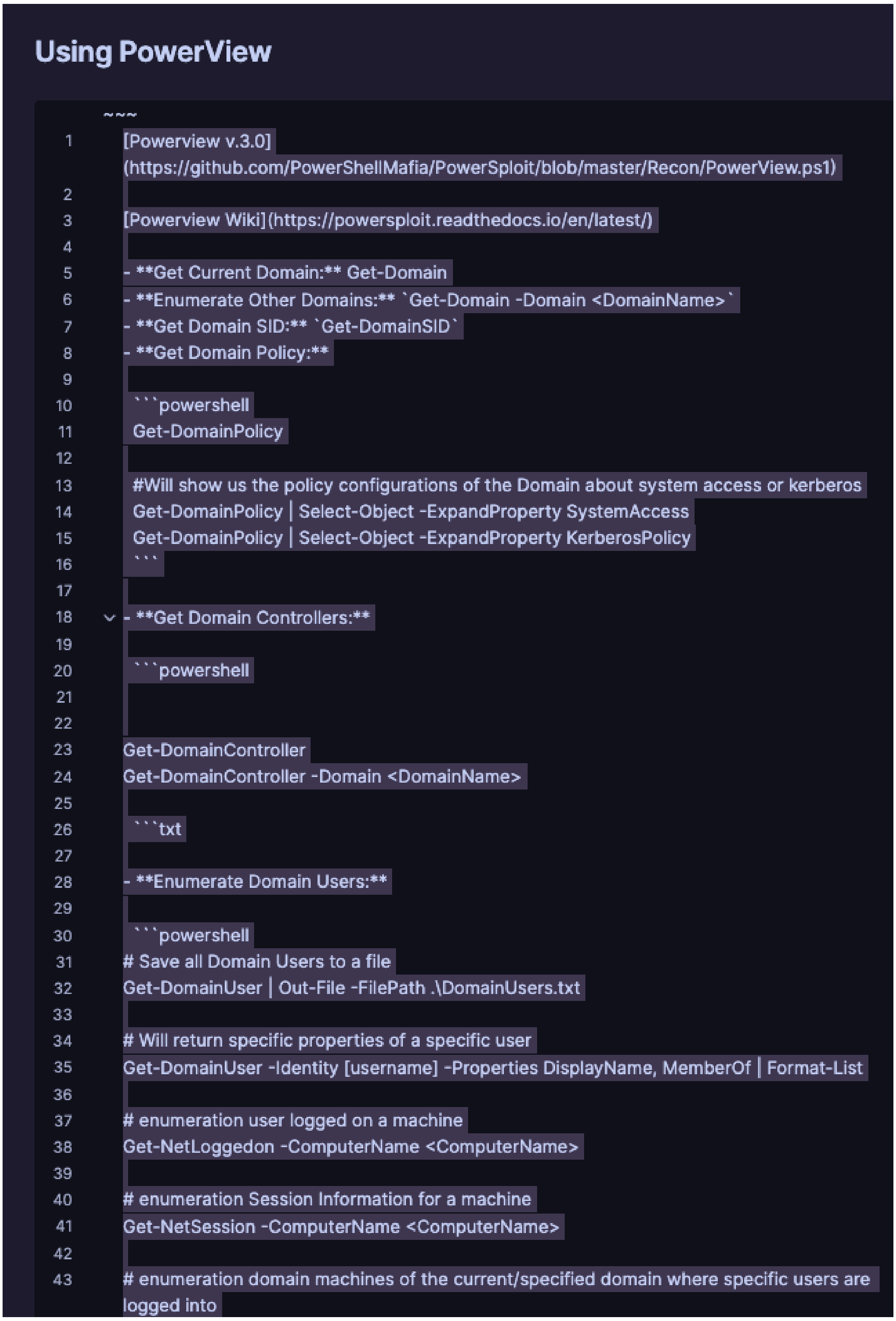
#Find computers were a Domain Admin OR a spesified user has a session
Find-DomainUserLocation | Select-Object UserName, SessionFromName

#Confirming admin access
Test-AdminAccess
```

Priv Esc to Domain Admin with User Hunting:
I have local admin access on a machine → A Domain Admin has a session on that machine → I steal his token and impersonate him → Profit!

Using AD Module

Then input three wave dashes ~. As you can see, the whole section is now contained within the wave dashes as a code block.



Using PowerView

````
~~~
[Powerview v.3.0]
(https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1)

[Powerview Wiki](https://powersploit.readthedocs.io/en/latest/)

- **Get Current Domain:** Get-Domain
- **Enumerate Other Domains:** `Get-Domain -Domain <DomainName>`
- **Get Domain SID:** `Get-DomainSID`
- **Get Domain Policy:**

 ```powershell
 Get-DomainPolicy

 #Will show us the policy configurations of the Domain about system access or kerberos
 Get-DomainPolicy | Select-Object -ExpandProperty SystemAccess
 Get-DomainPolicy | Select-Object -ExpandProperty KerberosPolicy
 ```

- **Get Domain Controllers:**

 ```powershell


Get-DomainController
Get-DomainController -Domain <DomainName>

 ```txt

- **Enumerate Domain Users:**

 ```powershell
# Save all Domain Users to a file
Get-DomainUser | Out-File -FilePath .\DomainUsers.txt

# Will return specific properties of a specific user
Get-DomainUser -Identity [username] -Properties DisplayName, MemberOf | Format-List

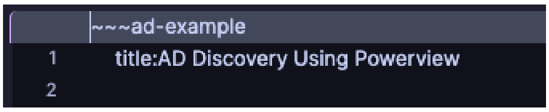
# enumeration user logged on a machine
Get-NetLoggedon -ComputerName <ComputerName>

# enumeration Session Information for a machine
Get-NetSession -ComputerName <ComputerName>

# enumeration domain machines of the current/specified domain where specific users are
logged into
````

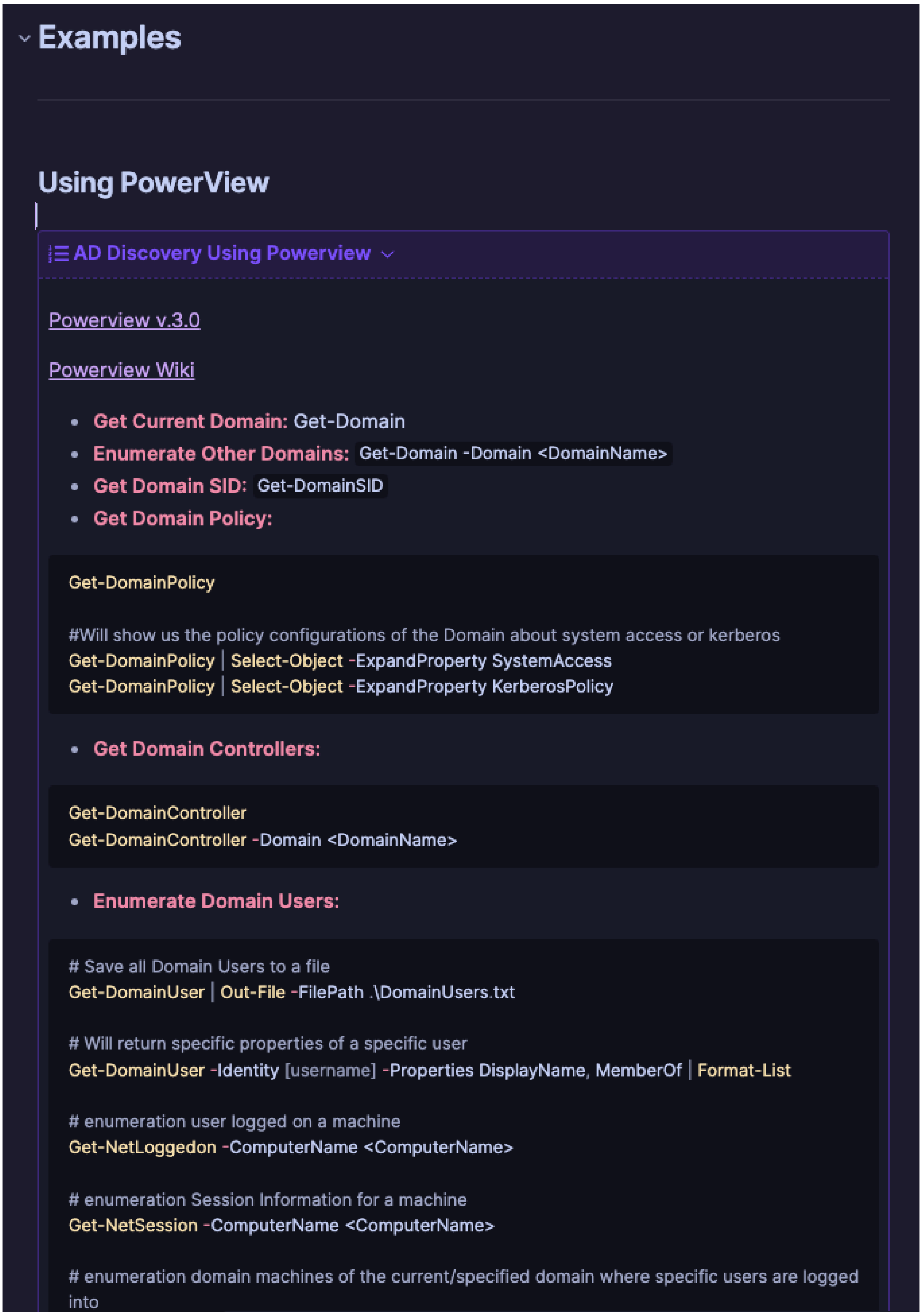
> If I used the Insert Codeblock command, the block would not work as intended.

Then you can add `ad-example` as the codeblock type. This will encapsulate the whole codeblock within an "example" admonition callout when previewing the note. Finally, add a title, such as "AD Discovery Using Powerview."



```
~~~ad-example
 title:AD Discovery Using Powerview

```
~~~



Examples

Using PowerView

AD Discovery Using Powerview

Powerview v.3.0

Powerview Wiki

- **Get Current Domain:** Get-Domain
- **Enumerate Other Domains:** `Get-Domain -Domain <DomainName>`
- **Get Domain SID:** `Get-DomainSID`
- **Get Domain Policy:**

```
Get-DomainPolicy

#Will show us the policy configurations of the Domain about system access or kerberos
Get-DomainPolicy | Select-Object -ExpandProperty SystemAccess
Get-DomainPolicy | Select-Object -ExpandProperty KerberosPolicy
```

- **Get Domain Controllers:**

```
Get-DomainController
Get-DomainController -Domain <DomainName>
```

- **Enumerate Domain Users:**

```
# Save all Domain Users to a file
Get-DomainUser | Out-File -FilePath .\DomainUsers.txt

# Will return specific properties of a specific user
Get-DomainUser -Identity [username] -Properties DisplayName, MemberOf | Format-List

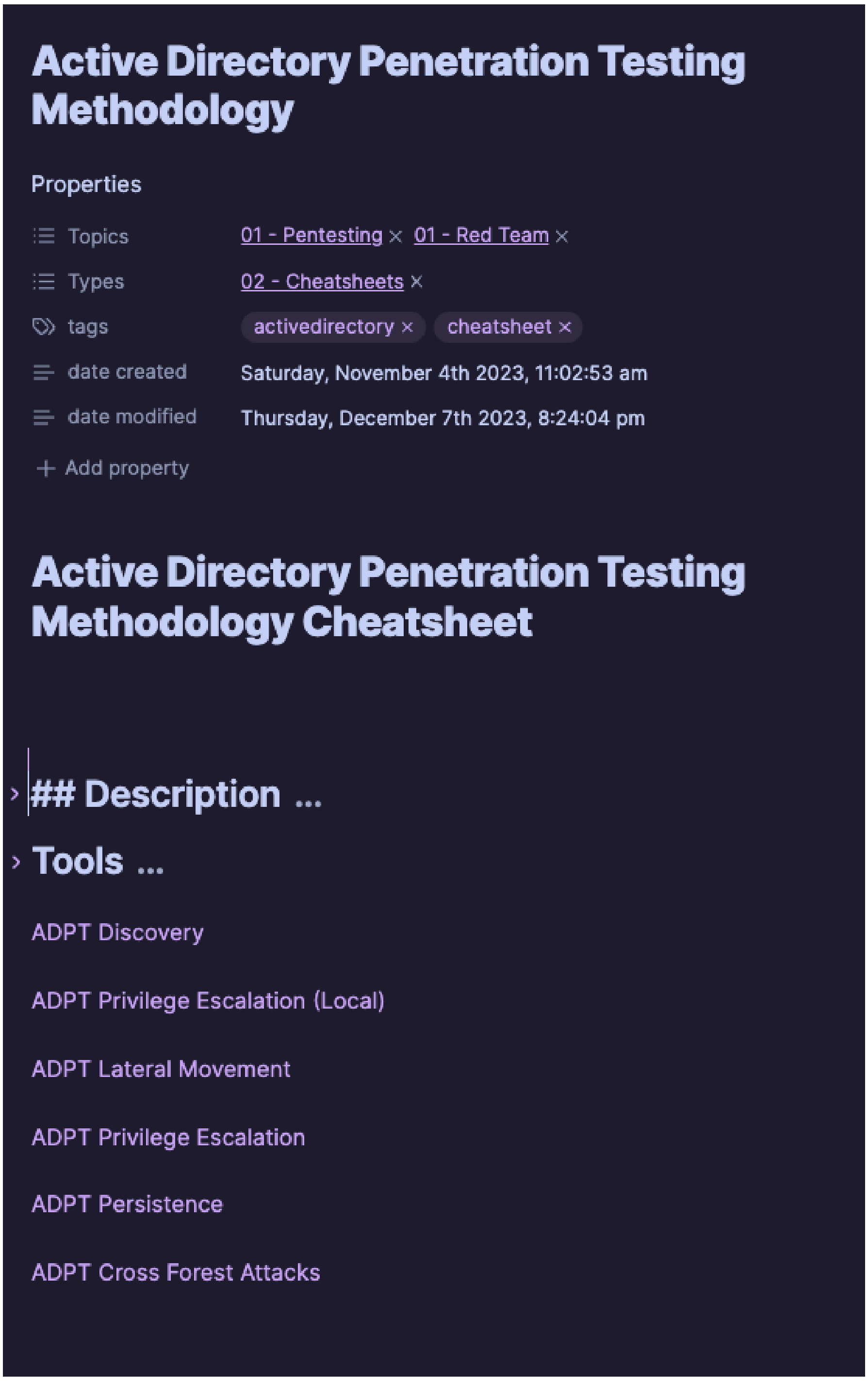
# enumeration user logged on a machine
Get-NetLoggedon -ComputerName <ComputerName>

# enumeration Session Information for a machine
Get-NetSession -ComputerName <ComputerName>

# enumeration domain machines of the current/specified domain where specific users are logged
into
```

I then performed the same callout encapsulation on the remaining "Examples" subheadings.

Going back to the parent note, rinse and repeat the whole process for each remaining heading.



Active Directory Penetration Testing Methodology

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Types	02 - Cheatsheets ×
tags	activedirectory × cheatsheet ×
date created	Saturday, November 4th 2023, 11:02:53 am
date modified	Thursday, December 7th 2023, 8:24:04 pm

+ Add property

Active Directory Penetration Testing Methodology Cheatsheet

› ## Description ...

› Tools ...

ADPT Discovery

ADPT Privilege Escalation (Local)

ADPT Lateral Movement

ADPT Privilege Escalation

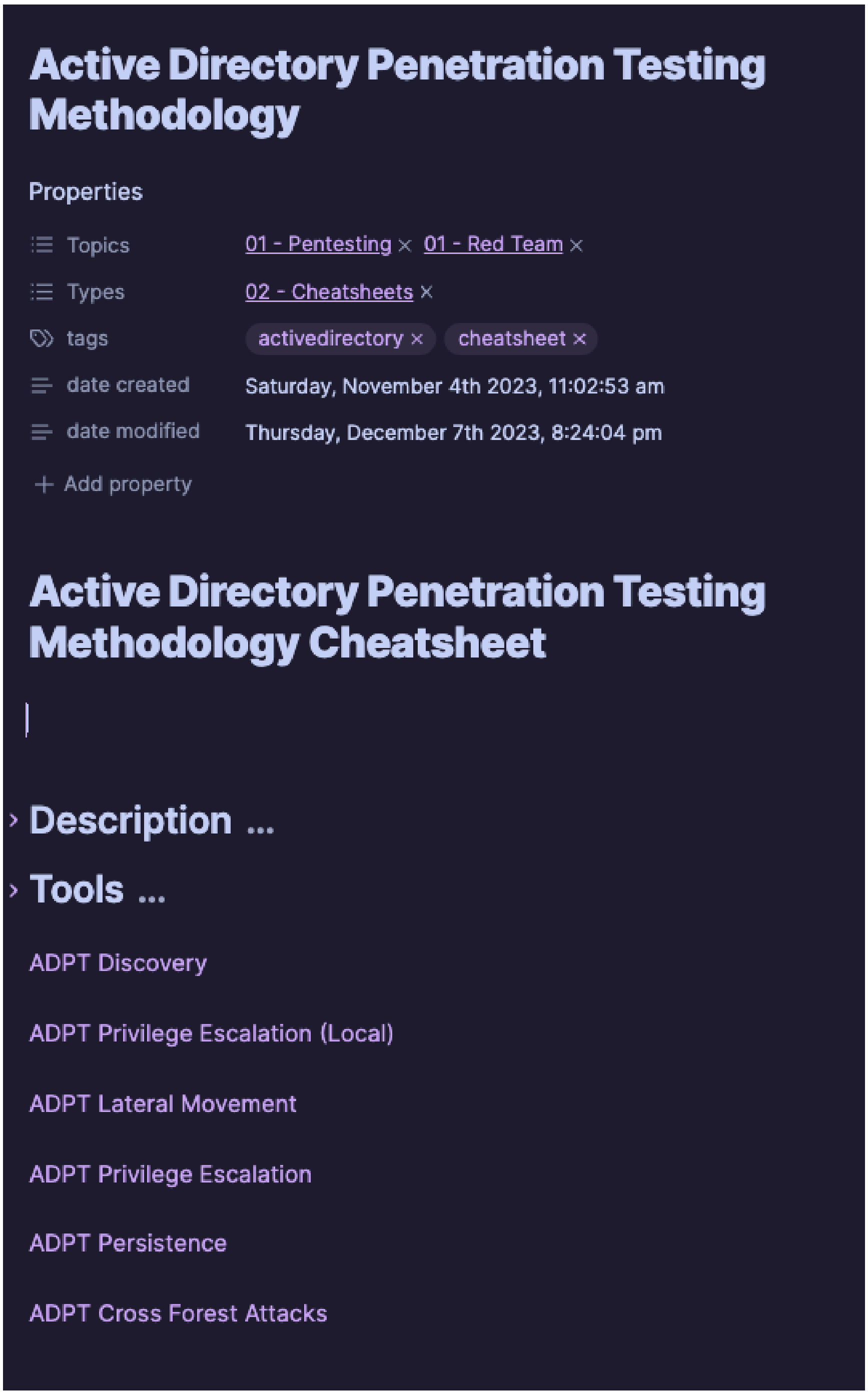
ADPT Persistence

ADPT Cross Forest Attacks

> This refactoring process can be somewhat tedious, but it will pay off later when you are referencing a technique during practice or a challenging exam, and every concept is logically organized with commands ready to be copied and pasted. Also, remember that if you are already using a parent note to encompass all child concepts, you won't have to do this whole refactoring process ever again.

7.2.6.4 Finishing the Parent Note

Going back to the parent note, we are left with an awkward structure that we will want to fix.



Active Directory Penetration Testing Methodology

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Types	02 - Cheatsheets ×
tags	activedirectory × cheatsheet ×
date created	Saturday, November 4th 2023, 11:02:53 am
date modified	Thursday, December 7th 2023, 8:24:04 pm

+ Add property

Active Directory Penetration Testing Methodology Cheatsheet

› Description ...

› Tools ...

ADPT Discovery

ADPT Privilege Escalation (Local)

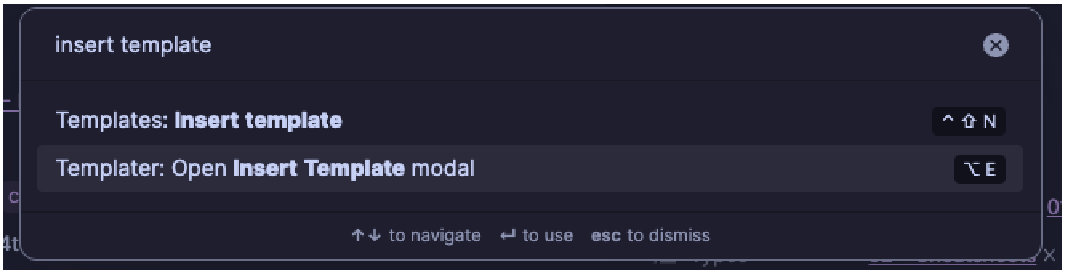
ADPT Lateral Movement

ADPT Privilege Escalation

ADPT Persistence

ADPT Cross Forest Attacks

Move your cursor to a blank space right after the main heading (as shown in the previous picture), and open up the command palette (`Cmd + P` or `Ctrl + P`). Select "Open Insert Template Modal" from Templater.

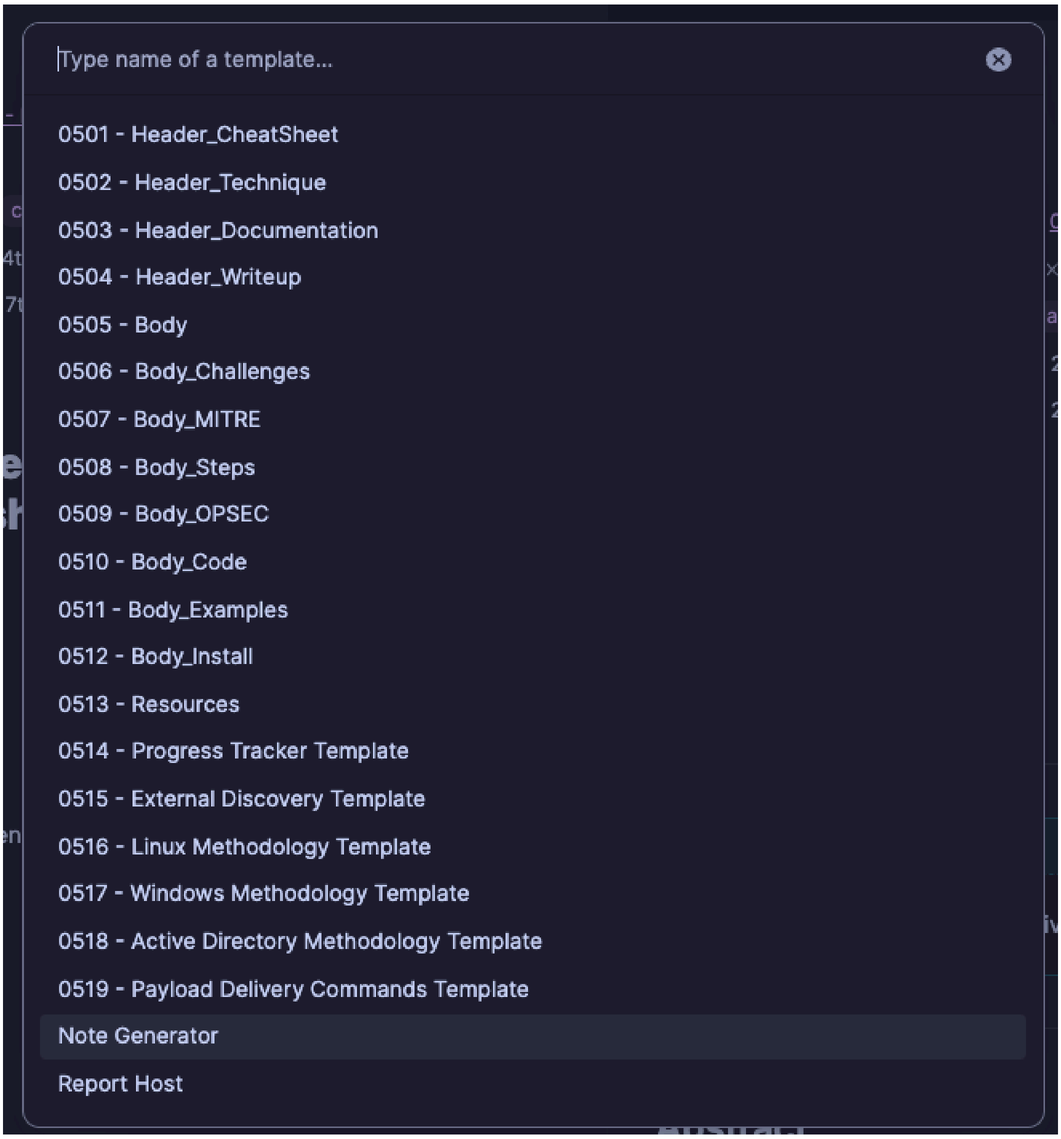


insert template

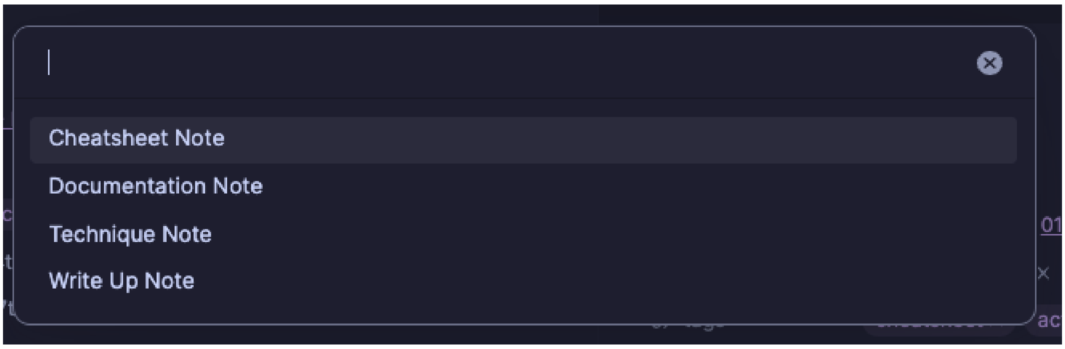
Templates: **Insert template** ^ ⇧ N

Templater: Open **Insert Template** modal ⌥ E

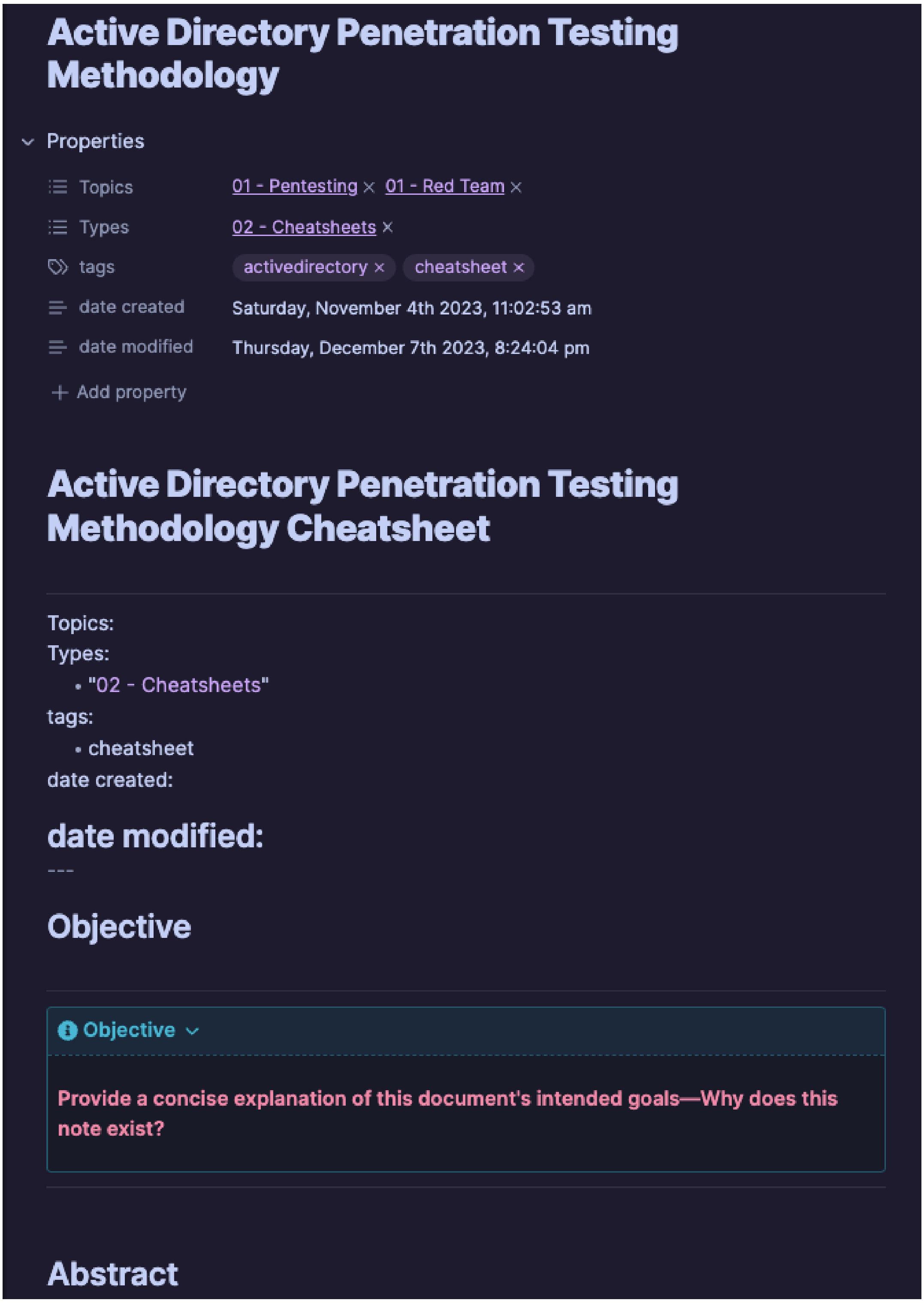
Choose the Note Generator.


Type name of a template...
0501 - Header_CheatSheet
0502 - Header_Technique
0503 - Header_Documentation
0504 - Header_Writeup
0505 - Body
0506 - Body_Challenges
0507 - Body_MITRE
0508 - Body_Steps
0509 - Body_OPSEC
0510 - Body_Code
0511 - Body_Examples
0512 - Body_Install
0513 - Resources
0514 - Progress Tracker Template
0515 - External Discovery Template
0516 - Linux Methodology Template
0517 - Windows Methodology Template
0518 - Active Directory Methodology Template
0519 - Payload Delivery Commands Template
Note Generator
Report Host

Then choose the corresponding note type (Cheatsheet in this case).



This will generate and insert a cheatsheet note into the current note.



Active Directory Penetration Testing Methodology

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Types	02 - Cheatsheets ×
tags	activedirectory × cheatsheet ×
date created	Saturday, November 4th 2023, 11:02:53 am
date modified	Thursday, December 7th 2023, 8:24:04 pm

+ Add property

Active Directory Penetration Testing Methodology Cheatsheet

Topics:
Types:

- "02 - Cheatsheets"

tags:

- cheatsheet

date created:

date modified:

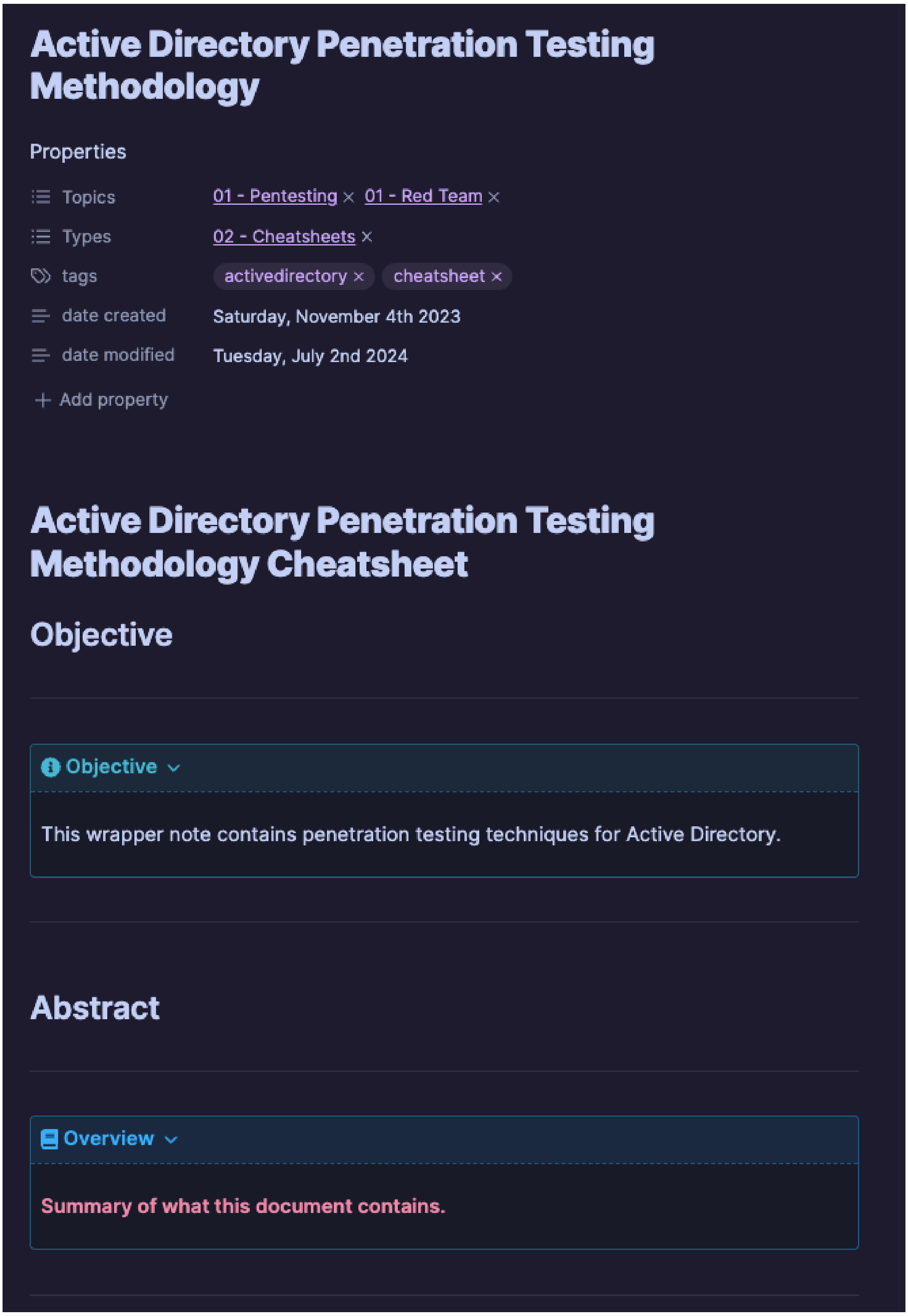
Objective

Objective

Provide a concise explanation of this document's intended goals—Why does this note exist?

Abstract

Remove the metadata section that got generated, lint the file (Cmd + Alt + L or Ctrl + Alt + L), and you are left with a new cheatsheet note.



Active Directory Penetration Testing Methodology

Properties

- Topics: 01 - Pentesting × 01 - Red Team ×
- Types: 02 - Cheatsheets ×
- tags: activedirectory × cheatsheet ×
- date created: Saturday, November 4th 2023
- date modified: Tuesday, July 2nd 2024

Active Directory Penetration Testing Methodology Cheatsheet

Objective

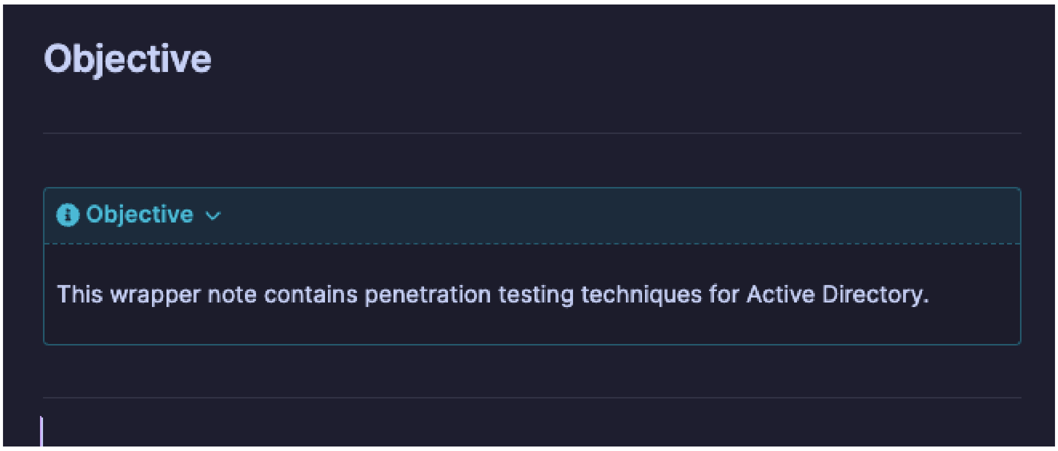
This wrapper note contains penetration testing techniques for Active Directory.

Abstract

Summary of what this document contains.

At this point, I would remove all sections, leaving only the "Objective" and "Resources" sections.

Fill in the "Objective" section.



Objective

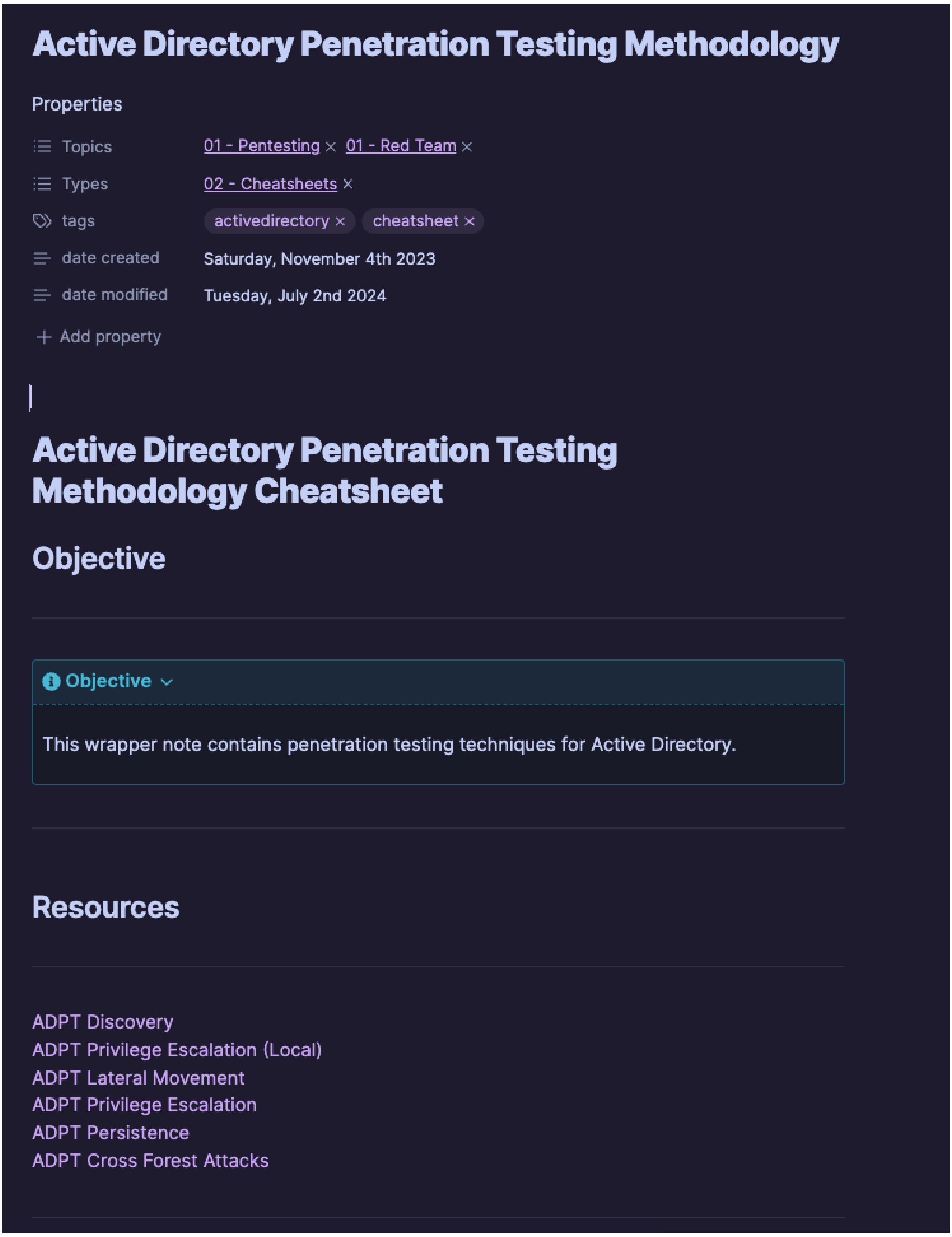
Objective

This wrapper note contains penetration testing techniques for Active Directory.

Move the children note's links to the Resources section.

7.2.6.5 Final Result

My final parent note looks like this:



Active Directory Penetration Testing Methodology

Properties

Topics: 01 - Pentesting × 01 - Red Team ×

Types: 02 - Cheatsheets ×

tags: activedirectory × cheatsheet ×

date created: Saturday, November 4th 2023

date modified: Tuesday, July 2nd 2024

+ Add property

Active Directory Penetration Testing Methodology Cheatsheet

Objective

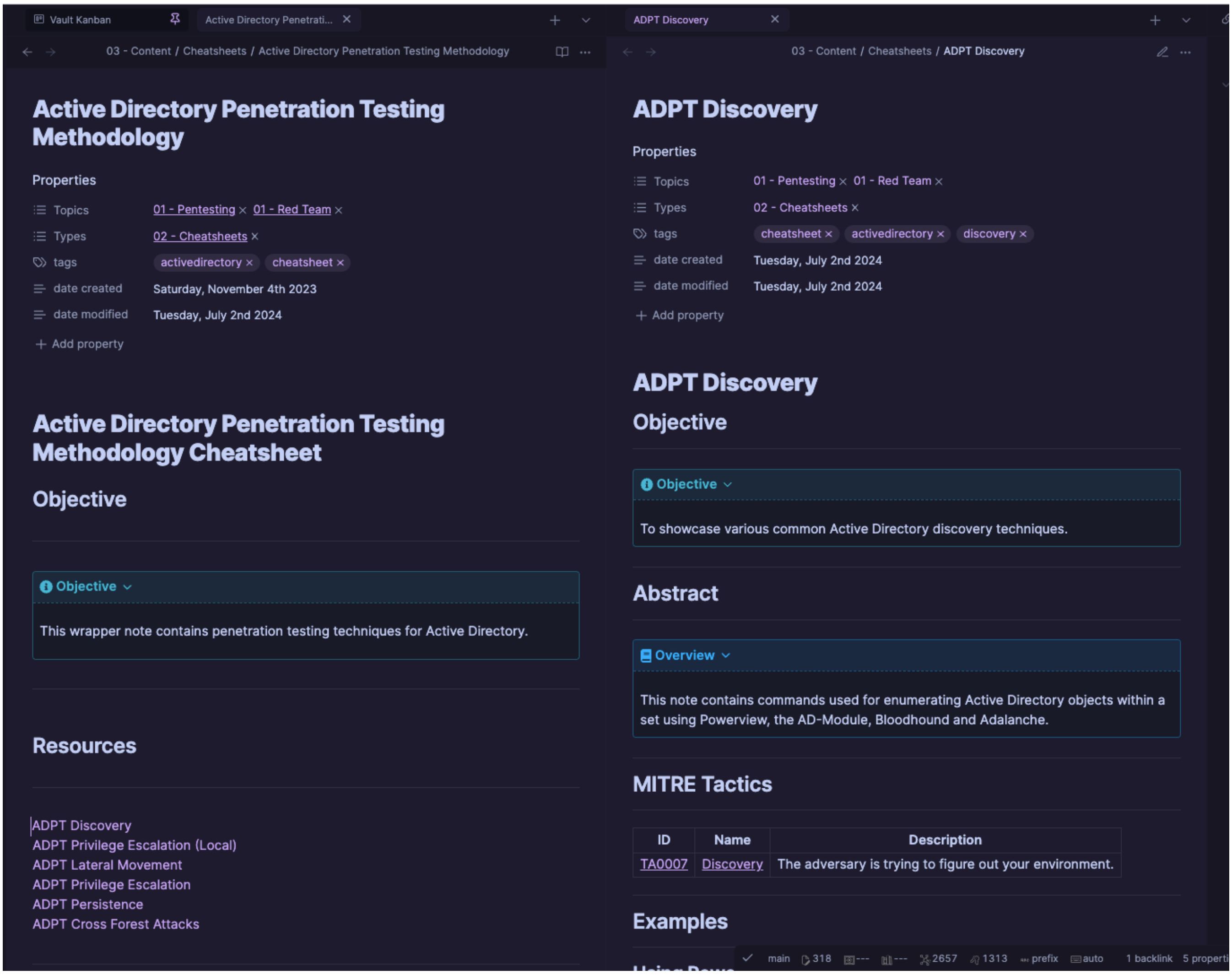
Objective

This wrapper note contains penetration testing techniques for Active Directory.

Resources

ADPT Discovery
ADPT Privilege Escalation (Local)
ADPT Lateral Movement
ADPT Privilege Escalation
ADPT Persistence
ADPT Cross Forest Attacks

Opening the parent/wrapper note (left) and children note (right):



03 - Content / Cheatsheets / Active Directory Penetration Testing Methodology

Active Directory Penetration Testing Methodology

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Types	02 - Cheatsheets ×
tags	activedirectory × cheatsheet ×
date created	Saturday, November 4th 2023
date modified	Tuesday, July 2nd 2024

+ Add property

Active Directory Penetration Testing Methodology Cheatsheet

Objective

Objective

This wrapper note contains penetration testing techniques for Active Directory.

Resources

ADPT Discovery
ADPT Privilege Escalation (Local)
ADPT Lateral Movement
ADPT Privilege Escalation
ADPT Persistence
ADPT Cross Forest Attacks

03 - Content / Cheatsheets / ADPT Discovery

ADPT Discovery

Properties

Topics	01 - Pentesting × 01 - Red Team ×
Types	02 - Cheatsheets ×
tags	cheatsheet × activedirectory × discovery ×
date created	Tuesday, July 2nd 2024
date modified	Tuesday, July 2nd 2024

+ Add property

ADPT Discovery

Objective

Objective

To showcase various common Active Directory discovery techniques.

Abstract

Overview

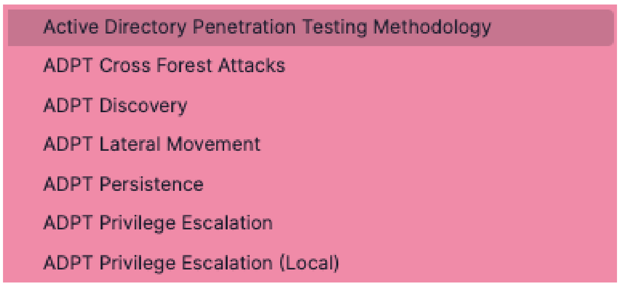
This note contains commands used for enumerating Active Directory objects within a set using Powerview, the AD-Module, Bloodhound and Adalanche.

MITRE Tactics

ID	Name	Description
TA0007	Discovery	The adversary is trying to figure out your environment.

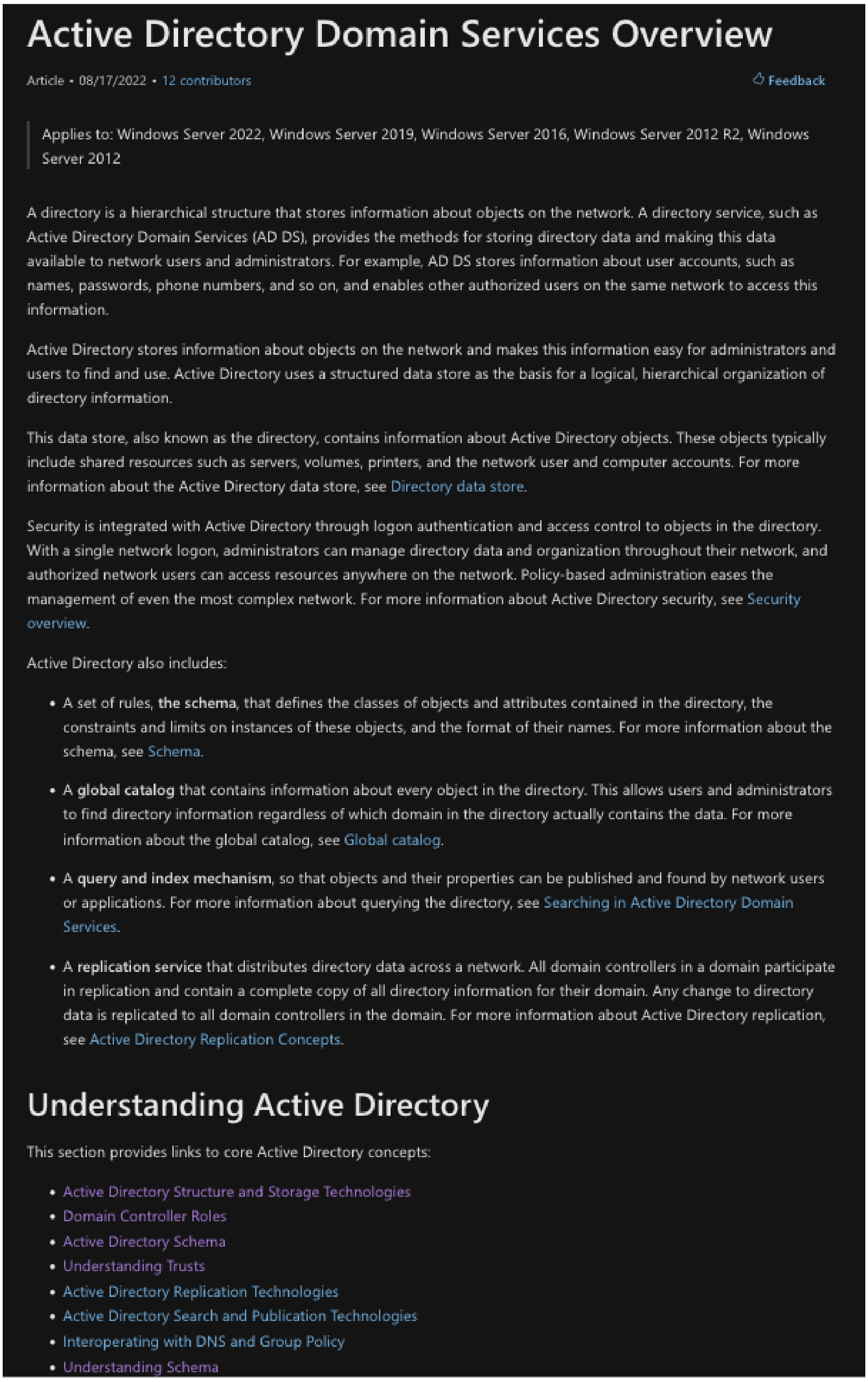
Examples

In my cheatsheets folder:


Active Directory Penetration Testing Methodology
ADPT Cross Forest Attacks
ADPT Discovery
ADPT Lateral Movement
ADPT Persistence
ADPT Privilege Escalation
ADPT Privilege Escalation (Local)

> This configuration mimics the way official documentation is presented on the internet.

If we go to Active Directory's documentation by Microsoft, we can see a similar structure. On this documentation page, they give an overview of what ADDS is and then provide a few links below so you can learn more about different topics.



Active Directory Domain Services Overview

Article • 08/17/2022 • 12 contributors

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

This data store, also known as the directory, contains information about Active Directory objects. These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts. For more information about the Active Directory data store, see Directory data store.

Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network. For more information about Active Directory security, see Security overview.

Active Directory also includes:

- A set of rules, **the schema**, that defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects, and the format of their names. For more information about the schema, see Schema.
- A **global catalog** that contains information about every object in the directory. This allows users and administrators to find directory information regardless of which domain in the directory actually contains the data. For more information about the global catalog, see Global catalog.
- A **query and index mechanism**, so that objects and their properties can be published and found by network users or applications. For more information about querying the directory, see Searching in Active Directory Domain Services.
- A **replication service** that distributes directory data across a network. All domain controllers in a domain participate in replication and contain a complete copy of all directory information for their domain. Any change to directory data is replicated to all domain controllers in the domain. For more information about Active Directory replication, see Active Directory Replication Concepts.

Understanding Active Directory

This section provides links to core Active Directory concepts:

- Active Directory Structure and Storage Technologies
- Domain Controller Roles
- Active Directory Schema
- Understanding Trusts
- Active Directory Replication Technologies
- Active Directory Search and Publication Technologies
- Interoperating with DNS and Group Policy
- Understanding Schema

7.2.7 Table of Contents

This plugin is very useful if you want to extract a note as a PDF for a report or if you simply want to add a table of contents to your finished note. These are my settings:

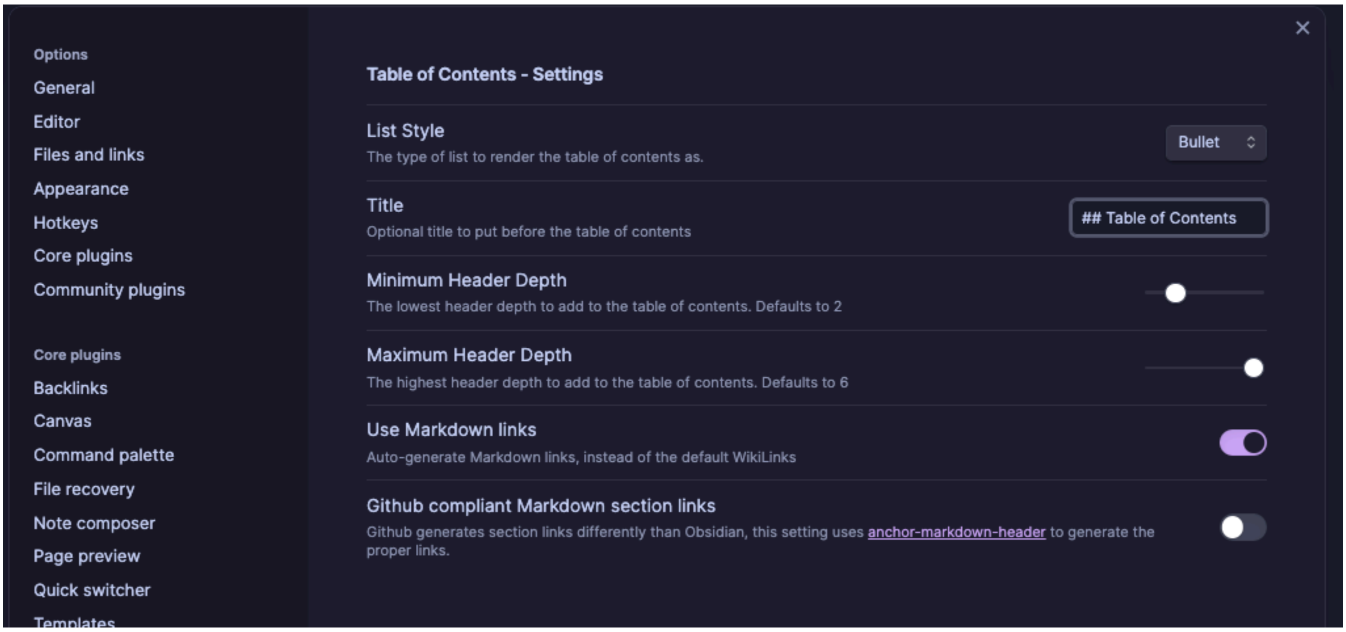


Table of Contents - Settings

List Style
The type of list to render the table of contents as.
Bullet

Title
Optional title to put before the table of contents
Table of Contents

Minimum Header Depth
The lowest header depth to add to the table of contents. Defaults to 2

Maximum Header Depth
The highest header depth to add to the table of contents. Defaults to 6

Use Markdown links
Auto-generate Markdown links, instead of the default WikiLinks

Github compliant Markdown section links
Github generates section links differently than Obsidian, this setting uses anchor-markdown-header to generate the proper links.

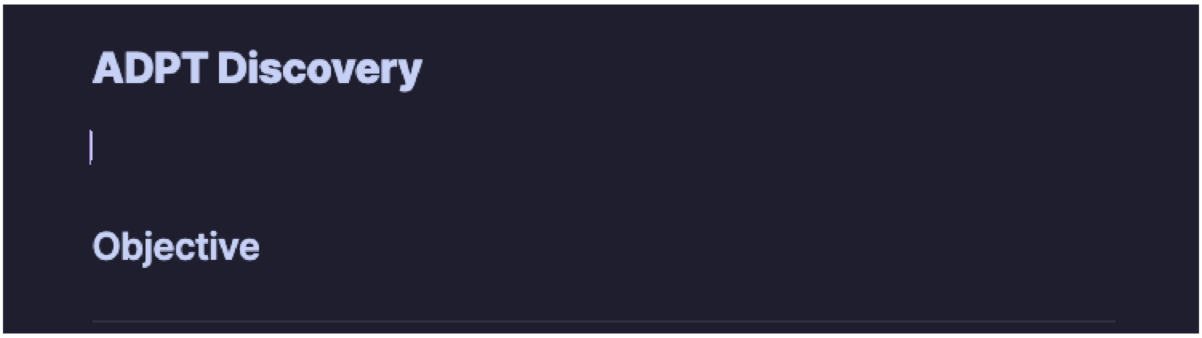
- List Style is bugged and only Bullet is available. When rendering, it will use a numbered list.
- Title is "## Table of Contents".
- Minimum Header Depth is 2.

> I suggest using your own preferred settings for this plugin. Experiment by tweaking Maximum and Minimum header depths.

7.2.7.1 Example Table of Contents

I will showcase an example using the "ADPT Discovery" note from the Note Refactor section.

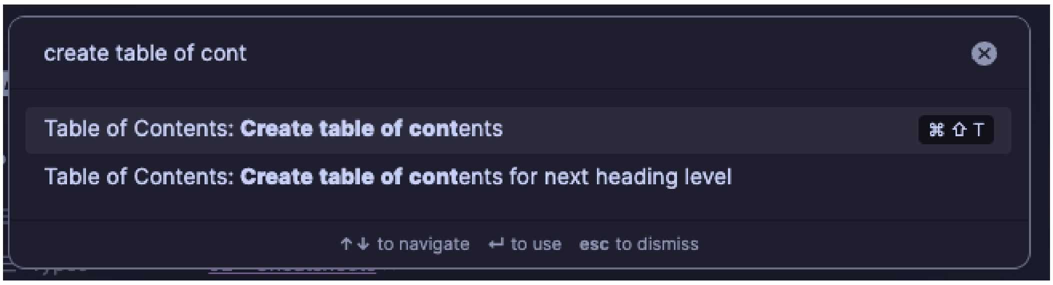
Say I want to extract this note into a PDF format. I would go to the line after the only level 1 heading, the main heading (containing the note's title and all content below).



ADPT Discovery

Objective

Open up the command palette and select *Create table of contents*:

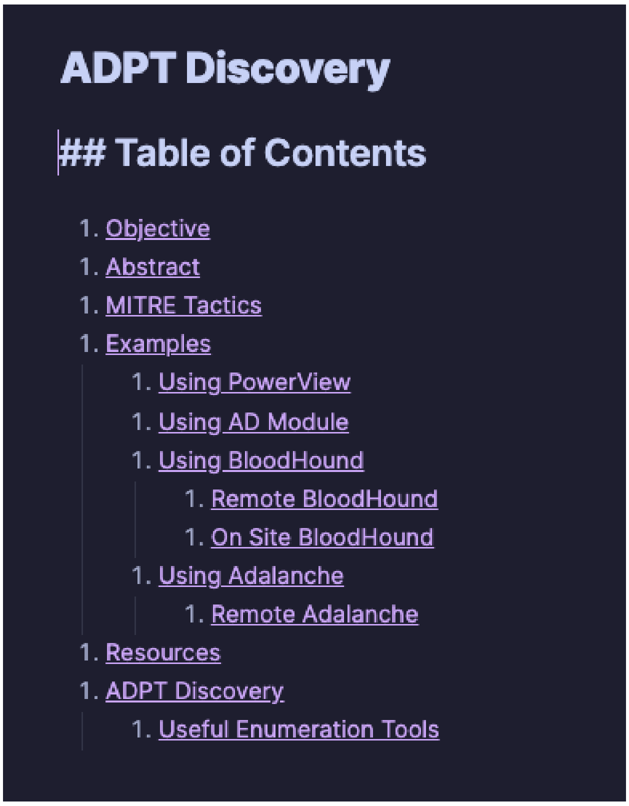


create table of cont

Table of Contents: **Create table of contents** ⌘ ⇧ T

Table of Contents: **Create table of contents** for next heading level

As you can see, a table of contents section gets generated:



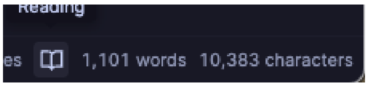
ADPT Discovery

Table of Contents

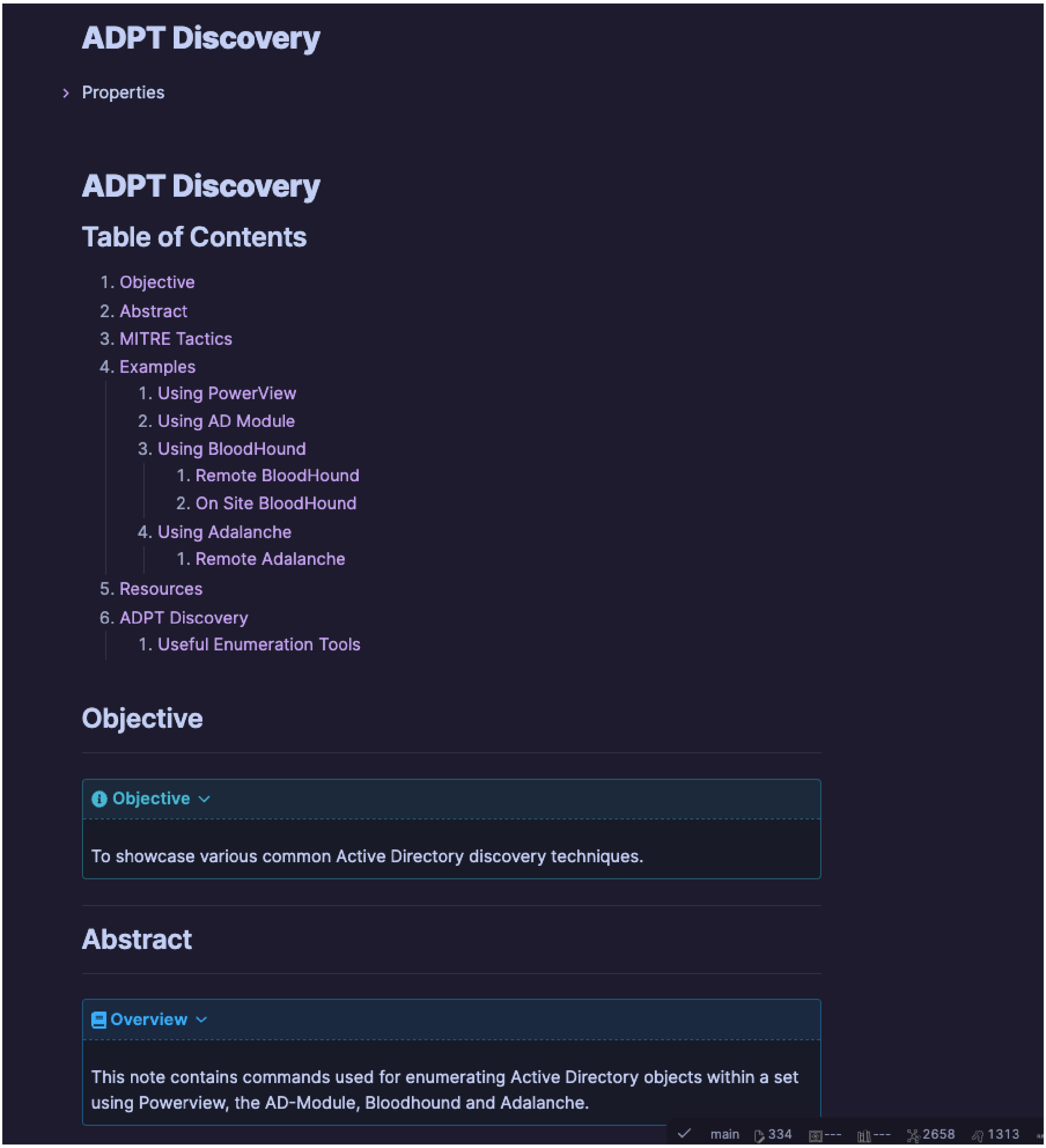
1. Objective
1. Abstract
1. MITRE Tactics
1. Examples
    1. Using PowerView
    1. Using AD Module
    1. Using BloodHound
        1. Remote BloodHound
        1. On Site BloodHound
    1. Using Adalanche
        1. Remote Adalanche
1. Resources
1. ADPT Discovery
    1. Useful Enumeration Tools

The numbers look wrong, but if we change to preview mode (Cmd + E or Ctrl + E), the numbers are displayed correctly.

> You can also change the display mode by clicking on the display mode icon in the status bar.



Reading mode representation:



ADPT Discovery

› Properties

ADPT Discovery

Table of Contents

Objective

Objective

To showcase various common Active Directory discovery techniques.

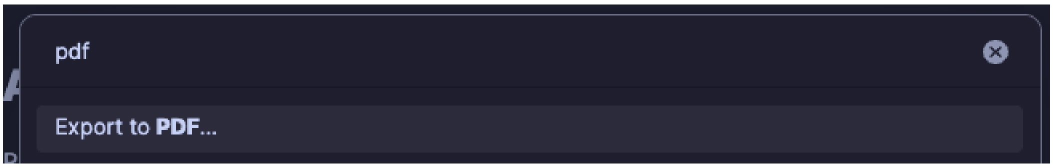
Abstract

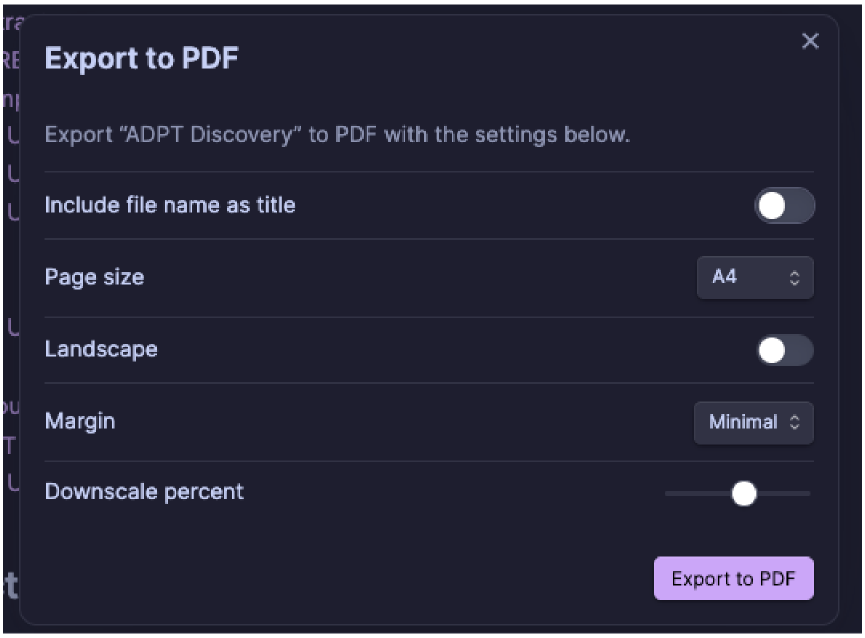
Overview

This note contains commands used for enumerating Active Directory objects within a set using Powerview, the AD-Module, Bloodhound and Adalanche.

The table of contents' links also work after exporting the note as a PDF:

Open up the command palette (`Cmd + P` or `Ctrl + P`) and select *Export to PDF*.





Export "ADPT Discovery" to PDF with the settings below.

Include file name as title ○

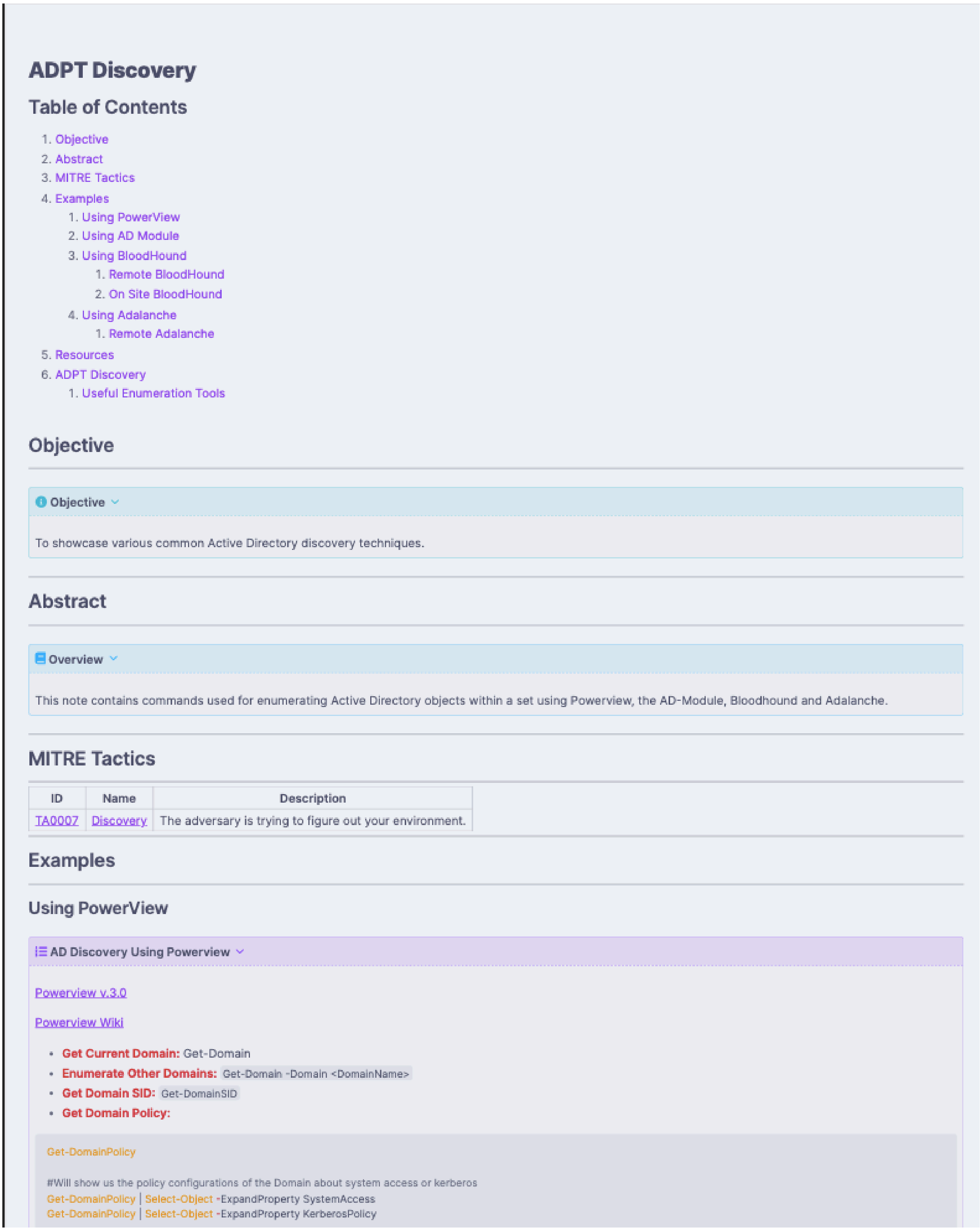
Page size: A4

Landscape ○

Margin: Minimal

Downscale percent

Final PDF note:



ADPT Discovery

Table of Contents

Objective

Objective

To showcase various common Active Directory discovery techniques.

Abstract

Overview

This note contains commands used for enumerating Active Directory objects within a set using Powerview, the AD-Module, Bloodhound and Adalanche.

MITRE Tactics

ID	Name	Description
TA0007	Discovery	The adversary is trying to figure out your environment.

Examples

Using PowerView

AD Discovery Using Powerview

Powerview v.3.0

Powerview Wiki

- **Get Current Domain:** Get-Domain
- **Enumerate Other Domains:** `Get-Domain -Domain <DomainName>`
- **Get Domain SID:** `Get-DomainSID`
- **Get Domain Policy:**

```
Get-DomainPolicy

#Will show us the policy configurations of the Domain about system access or kerberos
Get-DomainPolicy | Select-Object -ExpandProperty SystemAccess
Get-DomainPolicy | Select-Object -ExpandProperty KerberosPolicy
```

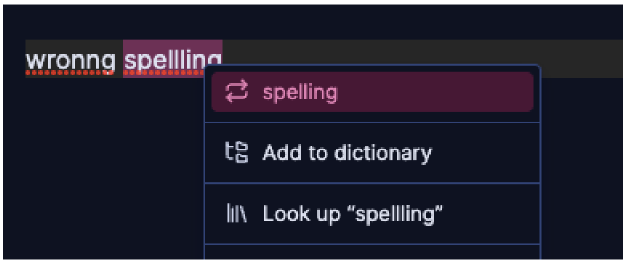
This is a very useful trick I use when converting markdown reports to PDF for certification exams.

> **Note**: I have found multiple bugs when using this plugin: TOC links do not work after rendering the PDF version, and the numbers in subsections are not displayed correctly when working in Live Preview mode from Obsidian.

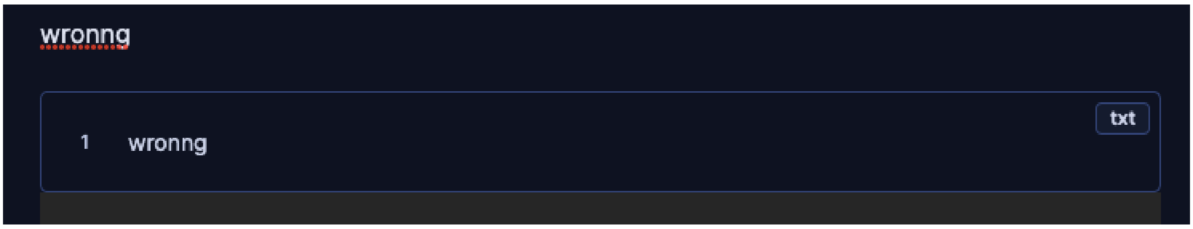
7.2.8 Various Complements

My settings are left as default, but I suggest going through this plugin's settings in case there is something you need to tweak.

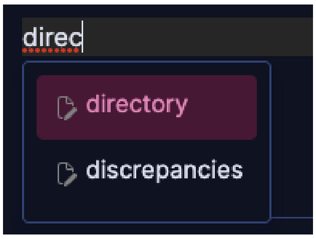
If you spell something wrong while working in Obsidian, the plugin will highlight that word. Then you can right-click the word and either add it to the dictionary or correct it using a suggestion.



By default, syntax highlighting is off when the word is inside a code block.



Another useful feature this plugin boasts is autocomplete suggestions as you type.



> As you can see, I use this plugin for those two settings exclusively. Feel free to experiment with the settings and let us know if you find any other cool tricks.