HOMELAND SECURITY
SYSTEMS ENGINEERING & DEVELOPMENT INSTITUTE™

Prepared for:
Department of Homeland Security

Decider 1.0.0

User Guide

Homeland Security

This document is a product of the Homeland Security Systems Engineering and Development Institute (HSSEDI™)

Contents

Introduction

Welcome to Decider

This guide is intended to walk analysts through the process of identifying MITRE ATT&CK® techniques and sub-techniques using Decider. We begin with a guided workflow and then proceed to identify alternative approaches to technique identification. We provide additional descriptions of Decider's features toward the end of the guide.

This project makes use of MITRE ATT&CK®

ATT&CK Terms of Use

CISA Best Practices for MITRE ATT&CK Mapping

The mapping steps below follow those identified in CISA's ATT&CK Mapping Guide. Analysts may choose their own starting point based on their familiarity with ATT&CK and the technical details / context available in the report.

1. Identify Tactics – Comb through the report to identify the adversary's tactics and the flow of the attack. To identify the tactics (the adversary's goals), focus on what the adversary was trying to accomplish and why.

Review the tactic definitions to determine how the identified behaviors might translate into a specific tactic. Each tactic includes a finite number of actions an adversary can take to implement their goal. Understanding the flow of the attack can help identify the techniques or sub-techniques that an adversary may have employed.

2. Identify Techniques – After identifying the tactics, review the technical details associated with how the adversary tried to achieve their goals. **Note**: if you have insufficient detail to identify an applicable technique, you will be limited to mapping to the tactic level, which alone is not actionable information for detection purposes.

Compare the behavior in the report with the description of the ATT&CK techniques listed under the identified tactic. If one of them matches, then it may be an appropriate technique. Be aware that multiple techniques may apply concurrently to the same behavior.

3. Identify Sub-techniques – Review sub-technique descriptions to see if they match the information in the report. A match here may be an appropriate sub-technique. Read sub-technique descriptions carefully to understand the differences between them. In cases where the parent of a sub-technique aligns to multiple tactics, make sure to choose the appropriate tactic. Note: map solely to the parent technique only if there is not enough context to identify a sub-technique.

Consider techniques and sub-techniques as elements of an adversary's playbook, rather than as isolated activities. Adversaries often use information they obtain from each activity in an operation to determine what additional techniques they will use next in the attack cycle. Because of this, techniques and sub-techniques are often linked in the attack chain.

Description of Decider

Decider is a web application that provides a series of questions to help analysts map threat reports to MITRE ATT&CK techniques. The decision tree starts at the Tactic level and flows through Techniques to Sub-Techniques. Analysts may also skip the decision tree by using the available search functionality. Decider provides features, such as suggesting related Techniques, warning about potential mis-mappings, and capturing the analyst's work in a shopping cart. The shopping cart feature allows the analyst to save their mapping progress. Carts can also be exported into JSON (for scripting usage / later importing), exported into ATT&CK Navigator layers (to visualize the attack heatmap in relation to defenses / existing adversary heatmaps), or a Microsoft Word Document report (where the mapped techniques and notes are in a table).

Troubleshooting

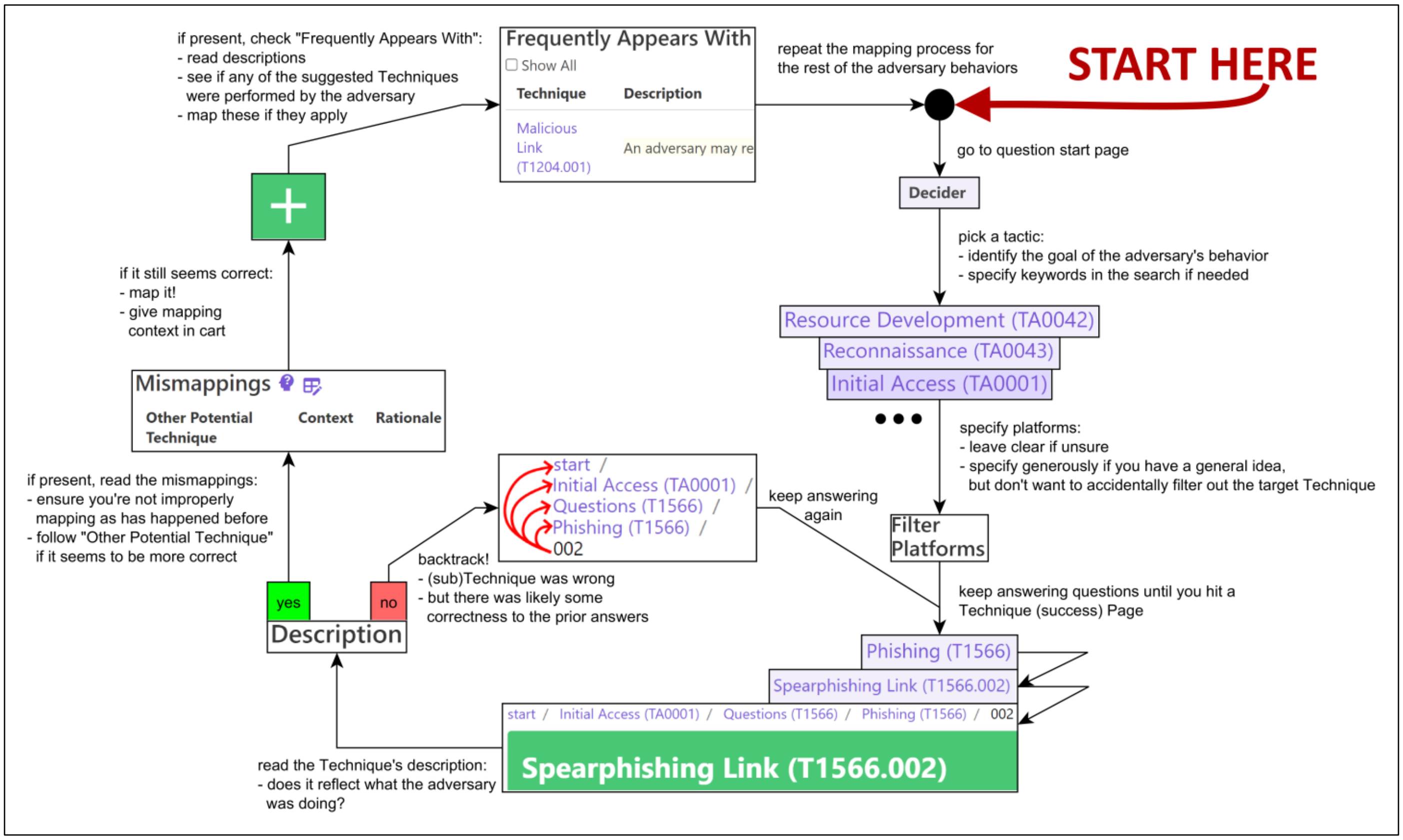
Please report any operational issues (.e.g., server not connecting, authentication failure, broken links, ambiguous or insufficient question content, information gaps in the guide, etc.), to dmounts@mitre.org. Suggestions for improvements to Decider are welcome as well.

Options for Analyst Workflows

Guided Workflow

1. Go to the main question page (*click **Decider** in the top-left*).
2. Identify the goal of the adversary's actions (Tactic) – click this card.
3. Identify what platform(s) the adversary's actions occurred on and set these filters accordingly.
4. Follow the prompts and select the best answer for each question.
5. You will ultimately reach a Technique page.
6. If the Technique appears to be correct, add it to the cart and you can include the related context in the text area of the cart.
7. If the Technique appears to be incorrect, backtrack through the steps.

Guided Mapping – Visual Workflow



START HERE
Decider
Resource Development (TA0042)
Reconnaissance (TA0043)
Initial Access (TA0001)
• • •
Filter Platforms
Phishing (T1566)
Spearphishing Link (T1566.002)
start / Initial Access (TA0001) / Questions (T1566) / Phishing (T1566) / 002
Spearphishing Link (T1566.002)
start / Initial Access (TA0001) / Questions (T1566) / Phishing (T1566) / 002
Description
yes
no
Mismappings
Other Potential Technique
Context
Rationale
Frequently Appears With
Show All
Technique
Description
Malicious Link (T1204.001)
An adversary may re

repeat the mapping process for the rest of the adversary behaviors

go to question start page

pick a tactic:
- identify the goal of the adversary's behavior
- specify keywords in the search if needed

specify platforms:
- leave clear if unsure
- specify generously if you have a general idea, but don't want to accidentally filter out the target Technique

keep answering questions until you hit a Technique (success) Page

read the Technique's description:
- does it reflect what the adversary was doing?

backtrack!
- (sub)Technique was wrong
- but there was likely some correctness to the prior answers

keep answering again

if present, read the mismappings:
- ensure you're not improperly mapping as has happened before
- follow "Other Potential Technique" if it seems to be more correct

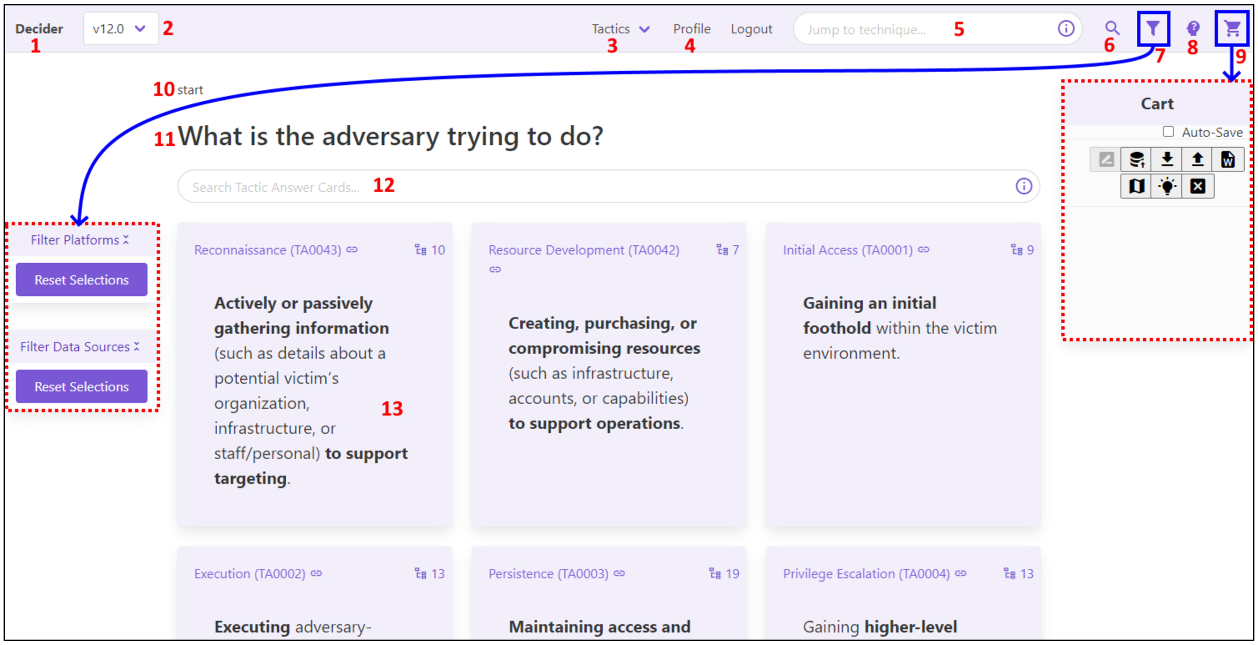
if it still seems correct:
- map it!
- give mapping context in cart

if present, check "Frequently Appears With":
- read descriptions
- see if any of the suggested Techniques were performed by the adversary
- map these if they apply

Note:
An analyst's ultimate workflow will be unique to them depending on their familiarity with ATT&CK and their level of experience in mapping adversary behaviors. Do whatever is most effective or intuitive for yourself. Take these suggestions as a means of familiarizing yourself with Decider navigation and discovery.

Navigating Decider

The Overview – General Features & Question Answering



What is the adversary trying to do?

Reconnaissance (TA0043) 10

Actively or passively gathering information (such as details about a potential victim's organization, infrastructure, or staff/personal) to support targeting.

Resource Development (TA0042) 7

Creating, purchasing, or compromising resources (such as infrastructure, accounts, or capabilities) to support operations.

Initial Access (TA0001) 9

Gaining an initial foothold within the victim environment.

Execution (TA0002) 13

Executing adversary-

Persistence (TA0003) 19

Maintaining access and

Privilege Escalation (TA0004) 13

Gaining higher-level

1. Home: Takes you to the main question page.

2. Version Selector: This dropdown allows you to change what version of ATT&CK content you are viewing across the website.

3. Tactics Dropdown: This dropdown contains the Tactic links. These links allow for quickly accessing the questions for each ATT&CK Tactic.

4. Profile: Gives access to self-password change, editing tools, and user management.

5. Mini Technique Search: Allows searching Techniques by name / ID. Clicking ⓘ will open information about this search. Aside from 6, this has a shortcut to the Full Search as well.

6. Open Full Search: This links to the Full Technique Search page.

7. Hide / Show Filters: Clicking this will toggle the visibility of the filters column on the left. Note: hiding the filters does nothing to clear or disable them – it's purely visual. The platform filters allow restricting displayed cards by what system(s) the adversary's behavior was against (e.g., Linux, Windows, …). The data sources filters allows restricting displayed cards by what types of data the sensors / logs are capable of collecting (e.g., Logon Session, Network Traffic, …). If no filters are selected, then all cards will be shown; otherwise, only cards that fulfil at least one specified filter will be shown (Platforms and Data Sources are handled in different filtering stages. So, if an entry is filtered out platform-wise, Data Sources cannot bring it back if a filter option there applies).

8. Help Documentation & Change Log: This opens a pop-up that allows you to open a local copy of this document – or – you can view a small log of the developmental changes over time (not comprehensive).

9. Hide/Show Cart: This button toggles the display of the cart of mapped Techniques. Here you can save the cart state to a file, restore an old cart file, export a Word table of Techniques, export an ATT&CK Navigator layer, gain insight on suggested Techniques to map based on currently mapped Techniques, or you can save a cart to the database to be reloaded later.

10. Breadcrumb Bar: Shows your location / progress in the process of answering questions. You can click the links here to navigate back to prior questions.

11. Current Question: This is the question you are currently trying to answer by selecting an answer card.

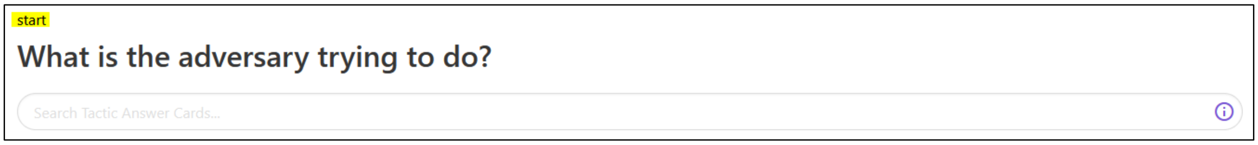
12. Answer Card Search: Searching keywords here will sort the answer cards by relevance and highlight where the terms appear on the card. Clicking ⓘ will open information about this search. This search is basic on the **start➔Tactics** page *(pictured)*, but more advanced on the **Tactic➔Techniques** and **Technique➔SubTechniques** pages.
Checkout "Answer Card Search – Basic vs Advanced" for more information.

13. Answer Cards: You click on one of these in order to answer the question at the top of the page - thus bringing you closer towards the Technique being described.

Answer Card Search – Basic vs Advanced

The capabilities of the answer card search depend on what page type you are on.

start➔Tactics page – basic search

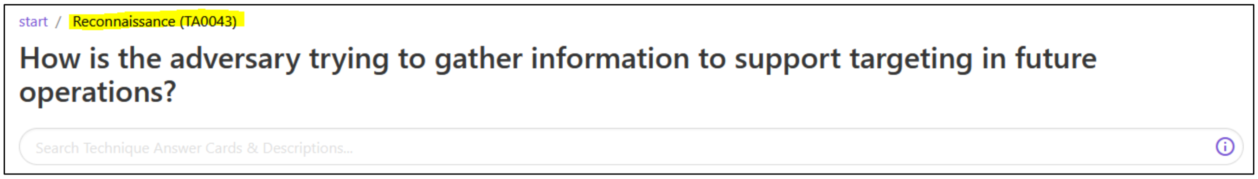


start

What is the adversary trying to do?

Search Tactic Answer Cards...

Tactic➔Techniques page – advanced search

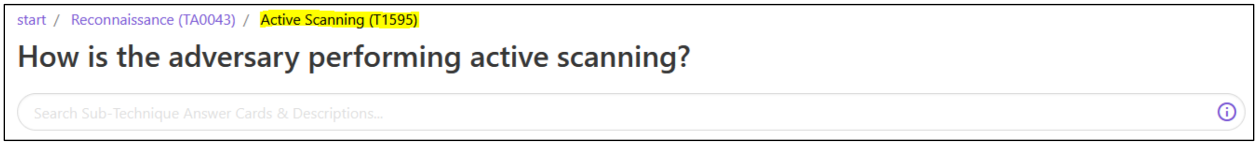


start / Reconnaissance (TA0043)

How is the adversary trying to gather information to support targeting in future operations?

Search Technique Answer Cards & Descriptions...

Technique➔SubTechniques page – advanced search



start / Reconnaissance (TA0043) / Active Scanning (T1595)

How is the adversary performing active scanning?

Search Sub-Technique Answer Cards & Descriptions...

Both advanced searches being mentioned here are exactly the same.
Note: the ⓘ icon has a different help screen for each of these two search types (basic vs advanced).
The help screen opened corresponds to the search currently being used for the page type you are on.

*Basic Answer Card Search (**start ➔Tactics**)*

This search only searches the content displayed on the answer cards themselves.
This is because there are a small number of Tactics (14) and they are all displayed at once.
This is essentially an alternative to [Ctrl]-[F].

While of limited utility – this search does support fuzziness and prefix-matching.

*Advanced Answer Card Search (**Tactic ➔Techniques, Technique ➔SubTechniques**)*

This search leverages more content than what is displayed on the answer cards.
This helps maintain searchability while allowing for a succinct answer card style.

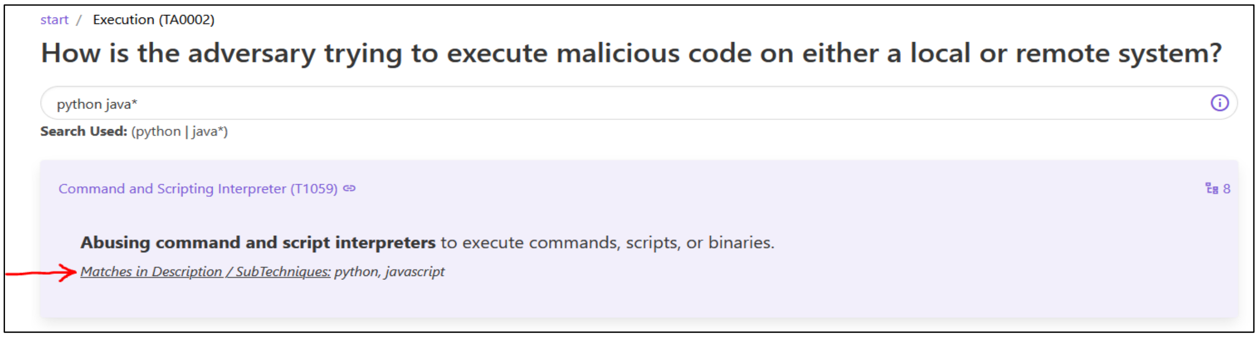
For a given answer card *(which represents a (Sub)Technique)* – these fields are searched:

- A**:** The answer card's content
- B**:** The Technique's description
- C**:** The answer card content of its SubTechniques *(if the card has SubTechs)*
- D**:** The description content of its SubTechniques *(if the card has SubTechs)*

The priority of each field (used in scoring / ordering results) is as follows: A **>** B **>** C **>** D.

When matches occur on fields that are not on the card content itself (ex: B, C, D)

- these matches will appear under the card content:



start / Execution (TA0002)

How is the adversary trying to execute malicious code on either a local or remote system?

python java*

Search Used: (python | java*)

Command and Scripting Interpreter (T1059)

Abusing command and script interpreters to execute commands, scripts, or binaries.

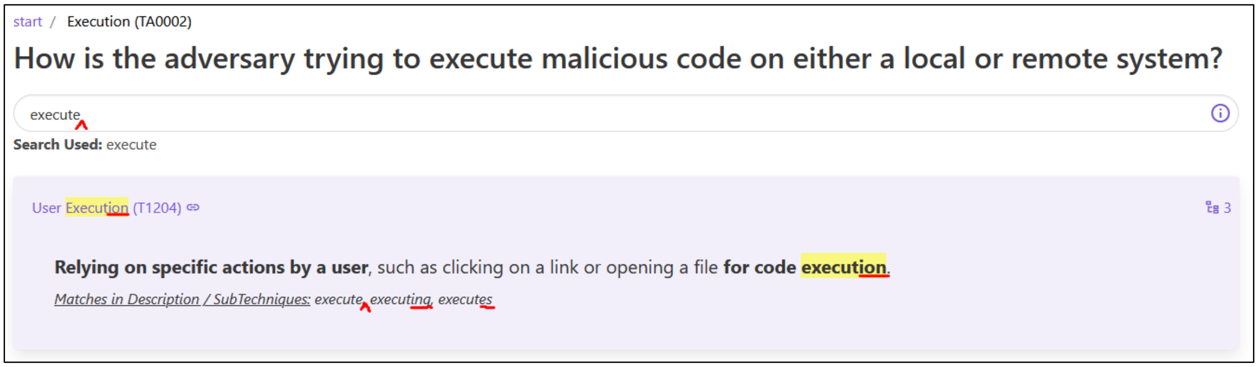
Matches in Description / SubTechniques: python, javascript

The advanced search supports boolean operators:

- Terms are **or**'ed together by default
- **()** are used for operation **order**
- **|** will **or**'s two expressions/terms together
- **&** will **and** two expressions/terms together
- **~** will **negate** the expression/term directly to the right of it (no spaces)
- ***** will make the expression/term directly to the left of it (no spaces) **prefix match**
- **""** are used to search for **phrases** containing any of the prior-mentioned operators
    - special characters get ignored, but, the order of each portion of A-z0-9 terms is enforced when matching the phrase

Word-stemming is automatically performed

- meaning that different endings to a search term are also matched / highlighted:



start / Execution (TA0002)

How is the adversary trying to execute malicious code on either a local or remote system?

execute

Search Used: execute

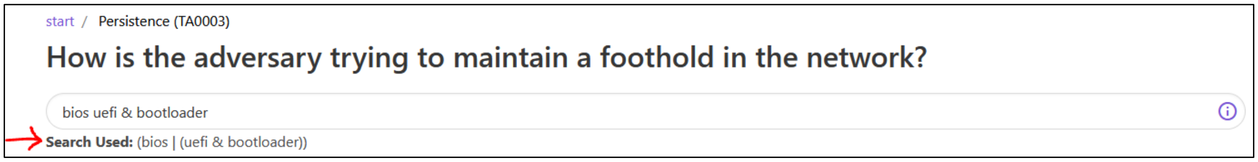
User Execution (T1204)

Relying on specific actions by a user, such as clicking on a link or opening a file **for code execution**.

Matches in Description / SubTechniques: execute, executing, executes

There is also a status area under the search bar

- **Search Used** describes how the server interpreted a given search
- the status area can also warn about malformed searches or say if the search yielded no results



start / Persistence (TA0003)

How is the adversary trying to maintain a foothold in the network?

bios uefi & bootloader

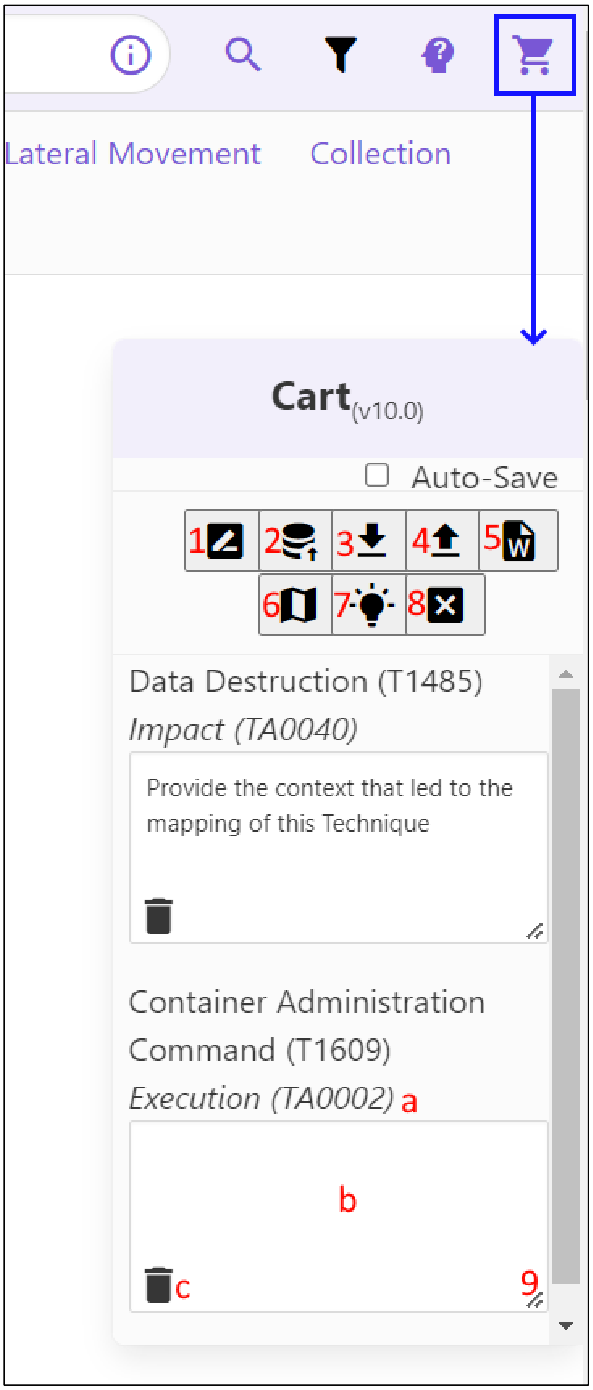
Search Used: (bios | (uefi & bootloader))

The limitation of this search is that **it cannot**:

- fuzzy match *(close-enough misspellings match anyway)*
- use synonyms *('execute' may imply 'run'/'process')*

Cart

Techniques are stored here to save progress during the mapping session.



1. Rename the Cart: Allows you to rename the cart.

2. Save to Database: This opens a pop-up that allows you to save the cart to the Decider database for later usage. The cart can be saved as a new report, or you can overwrite an existing report as to update it with the new work. "cart" and "report" are essentially the same here, reports are just carts that are saved to the database.

3. Save a Copy of The Cart: Allows you to save a copy of the cart locally as a JSON file.

4. Import data into the cart: Takes a previously downloaded JSON file and populates the cart.

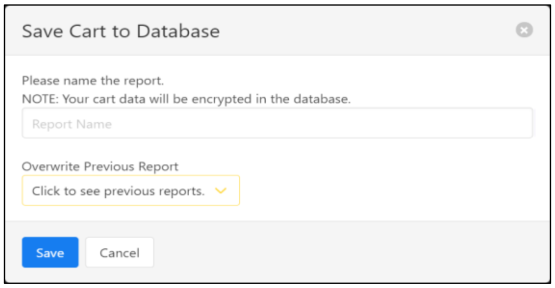
These two serve as a means of saving mapping progress locally between sessions, while the database button serves as a centralized means to do so.

5. Export to Word Doc: Downloads a Word document containing a table of the mapped Techniques.

6. Export to Navigator: Exports the cart to an ATT&CK Navigator JSON that can be used at https://mitre-attack.github.io/attack-navigator/

7. Suggested Techniques *(cart wide)*: Gives suggestions of Techniques to map based on cart contents.

8. Close cart: Deletes all entries in the cart.



Save Cart to Database

Please name the report.
NOTE: Your cart data will be encrypted in the database.

Report Name

Overwrite Previous Report

Click to see previous reports.

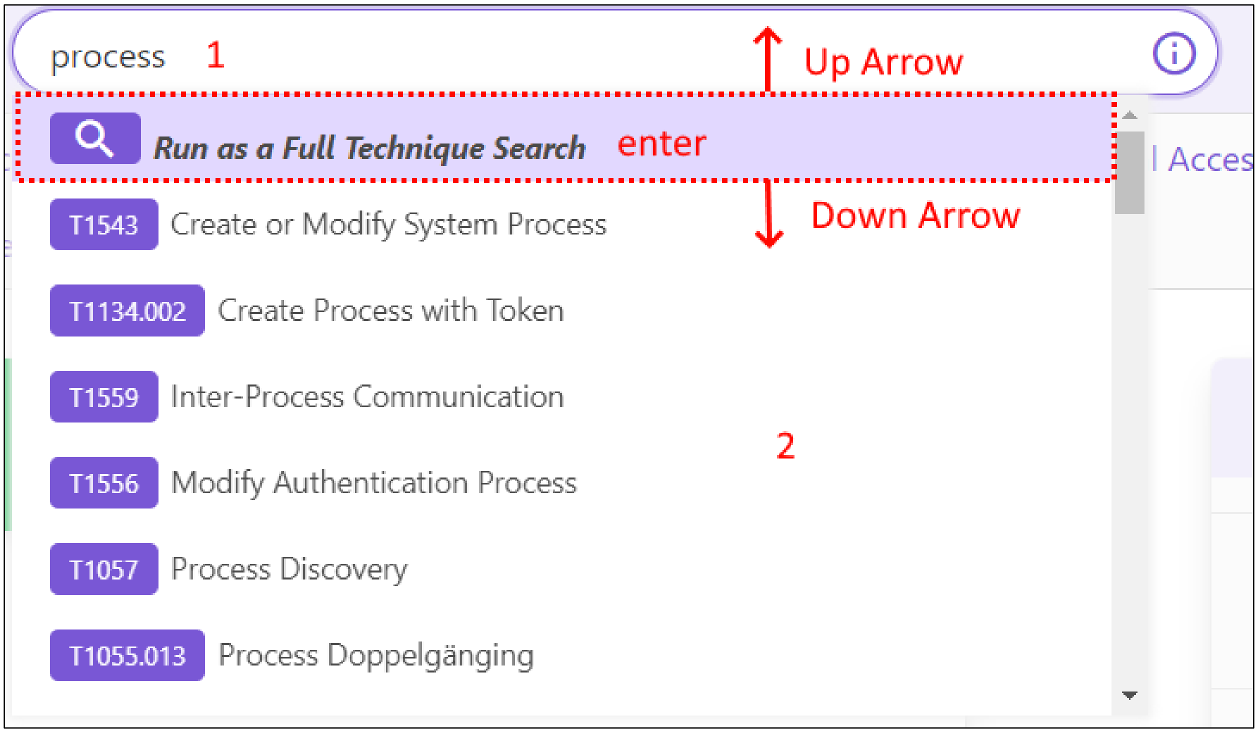
Save Cancel

9. Cart Entry: This is how a mapped Technique is displayed in the cart.

- **a. Mapped Technique & Its Tactic:** This is also a link to the Technique detail page.
- **b. Mapping Comment:** Here you can include text explaining why this Technique was mapped.
- **c. Delete Entry:** Deletes this single cart entry.

Mini Technique Search

Allows for quickly jumping to Technique pages by Technique name or ID.

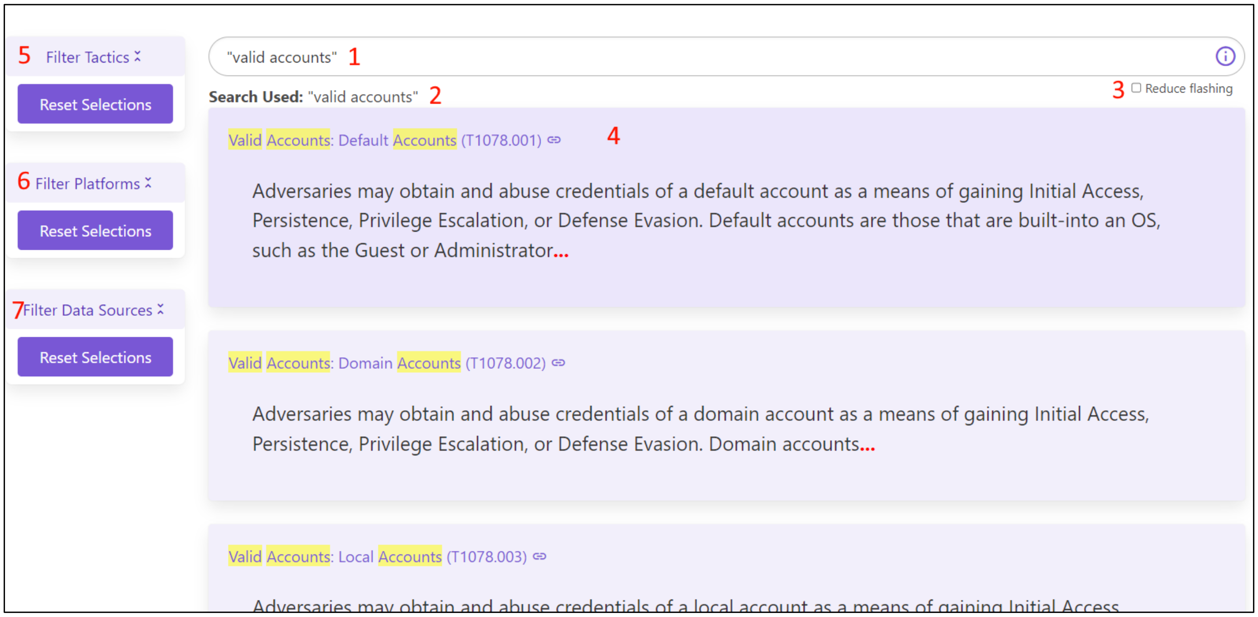

process
1
Up Arrow
Run as a Full Technique Search
enter
Down Arrow
T1543 Create or Modify System Process
T1134.002 Create Process with Token
T1559 Inter-Process Communication
2
T1556 Modify Authentication Process
T1057 Process Discovery
T1055.013 Process Doppelgänging
| Acces

1. Search Area: Enter a Technique Name or ID here and results will appear automatically. Clicking ⓘ will open information about this search.

2. Results: Click an entry to go to its page. You can also use the **[up-arrow]**, **[down-arrow]**, and **[enter]** keys as an alternative means of navigation.

Full Technique Search

The following describes a full-text search process for Techniques, along with filtering options.



Search Used: "valid accounts"

Valid Accounts: Default Accounts (T1078.001)

Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator...

Valid Accounts: Domain Accounts (T1078.002)

Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts...

Valid Accounts: Local Accounts (T1078.003)

Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access

1. Search Area: Enter a search query – results will update automatically.

Clicking ⓘ will open information about this search.

This search supports prefix-matching, boolean logic, requiring specific phrases, and it automatically stems words *(process = processes = processing = processed)*.

Note: This search does not allow searching for symbols – all non A-Za-z0-9 / space characters get replaced with spaces, and that result is used as the search query. Any terms that get split by this will be turned into phrases – so all parts of the term must appear in the search result card.

For Example: hklm\system → "hklm system"

Quotes serve another purpose outside of phrases, they allow one to enter a term that contains any of the special characters (but not quotes): **&**, **|**, **~**, **(**, **)**, *****.

2. Search Used: This provides transparency as to how Decider's search is interpreting your query. It prevents confusion if a special character is used, or if there is an issue with the search itself.

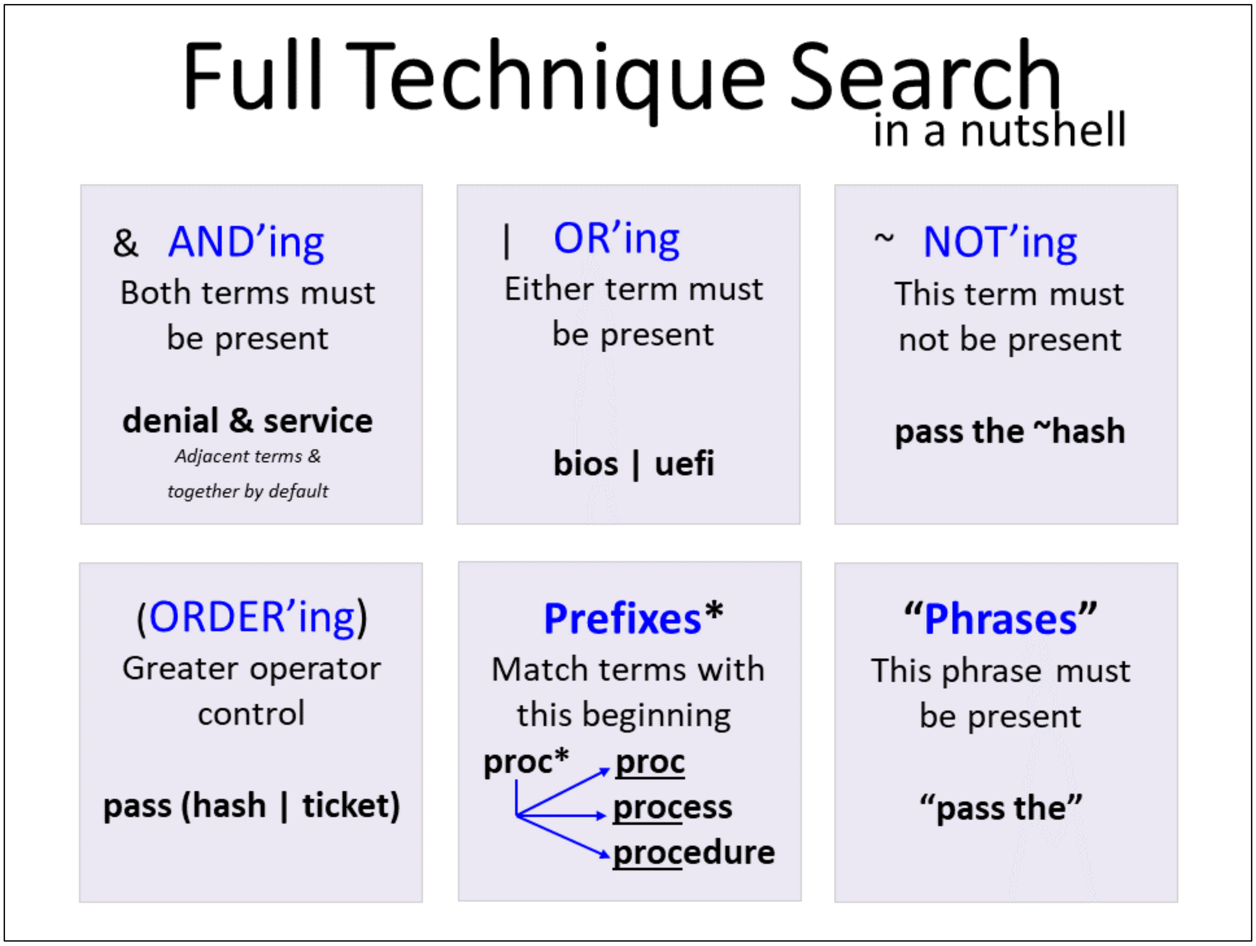
3. Reduce Flashing: When checked – this will set the background of the results area to the same pastel purple as the result cards. This removes the flashing that can occur with the white <-> purple transitioning as matching results come and go.

4. Results: Click a Technique to go to its page – matched terms are highlighted and a few snippets with the matched terms are shown.

5. Tactic Filtering: None selected: Techniques having any Tactic as their parent are shown. Selections made: only Techniques having any of the selected Tactics as their parent(s) are shown.

6. **Platform Filtering:** None selected: Techniques that run on any platform are shown. Selections made: only Techniques that run on any of the selected platforms are shown.

7. **Data Source Filtering**: None selected: Techniques that can be detected using any type of data source / collected data are shown. Selections made: only Techniques that are identifiable using the selected data sources are shown.



Full Technique Search

in a nutshell

& AND'ing

Both terms must be present

denial & service

Adjacent terms & together by default

| OR'ing

Either term must be present

bios | uefi

~ NOT'ing

This term must not be present

pass the ~hash

(ORDER'ing)

Greater operator control

pass (hash | ticket)

Prefixes*

Match terms with this beginning

proc*

proc
process
procedure

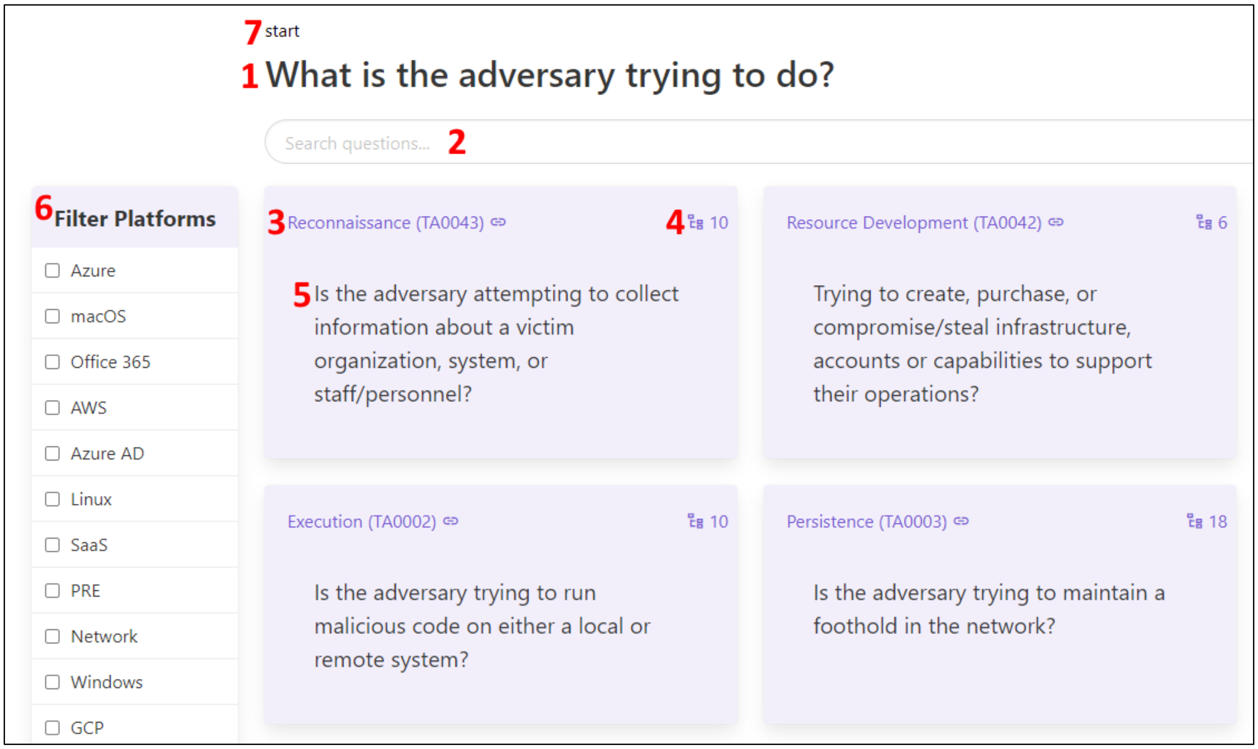
"Phrases"

This phrase must be present

"pass the"

Searches from the (Main) Question Page

Start the question-answer process by picking a Tactic.
Other question pages are essentially the same – except you pick between (sub)Techniques instead.



start

What is the adversary trying to do?

Search questions...

Filter Platforms

☐ Azure
☐ macOS
☐ Office 365
☐ AWS
☐ Azure AD
☐ Linux
☐ SaaS
☐ PRE
☐ Network
☐ Windows
☐ GCP

Reconnaissance (TA0043) 10

Is the adversary attempting to collect information about a victim organization, system, or staff/personnel?

Resource Development (TA0042) 6

Trying to create, purchase, or compromise/steal infrastructure, accounts or capabilities to support their operations?

Execution (TA0002) 10

Is the adversary trying to run malicious code on either a local or remote system?

Persistence (TA0003) 18

Is the adversary trying to maintain a foothold in the network?

1. Question: Prompt that you need to answer by selecting a card.

2. Answer Card Search: Entering keywords here will order the cards by relevance. Search terms are also highlighted on the cards. See "Answer Card Search – Basic vs Advanced" for more info.

3. Answer Card – ATT&CK Link: You can click here to open the ATT&CK page for the answer card.

4. Child Count: Shows the number of cards that will appear after clicking this one.

For a Tactic, this shows the number of Techniques under that Tactic.

For a Technique, this shows the number of Sub-Techniques under that Technique.

When this is 0, clicking the card will take you to the Technique (Success) Page.

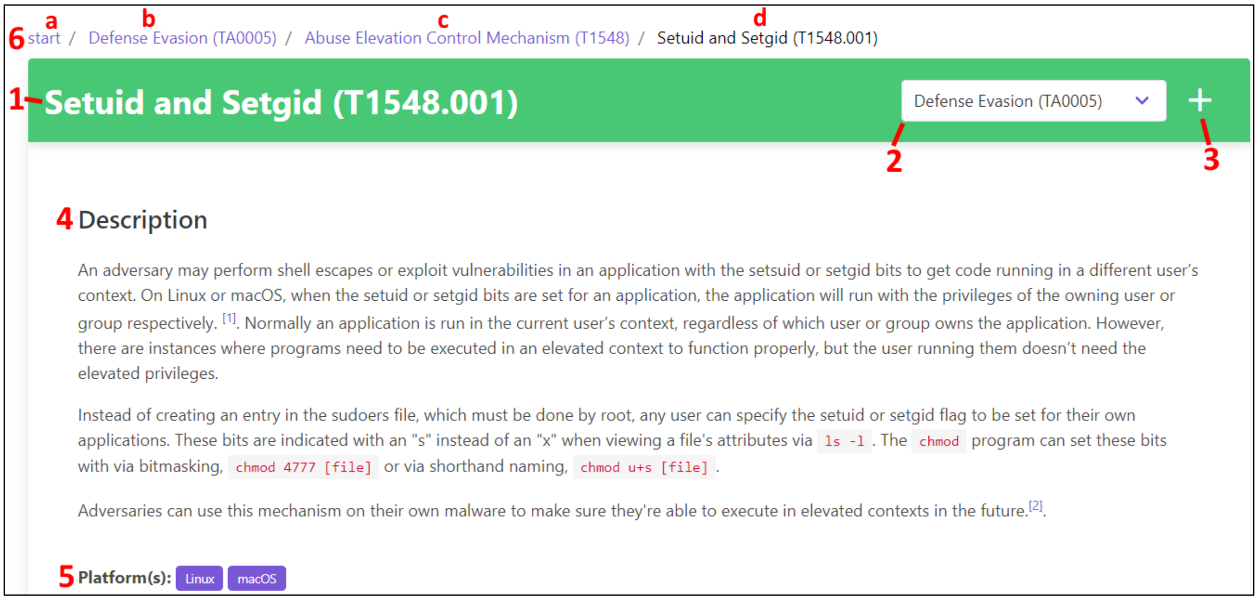
5. Answer Card – Answer Link: You select a card and progress by clicking its answer. (*Clicking anywhere on the card that isn't the ATT&CK link also works*).

6. Platform Filtering: No selections: all cards will be shown. Selections made: only cards that lead to Techniques that run on any of the specified platforms will be shown.
(not shown in this image, but Data Source filtering is below the Platform filtering.
it is explained in detail above in *The Overview – General Features & Question Answering*).

7. Crumb Bar: While present on all question pages and all Technique pages – the crumb bar is inherently uninteresting on the main question page. See *Reaching the Technique (Success) Page* for a demonstration of all components in a crumb bar.

Reaching the Technique (Success) Page

After enough questions have been answered – you will end up on a page for the (Sub)Technique to be mapped. Since this page is larger, it will be broken into multiple screenshots (in the same order as they appear in the tool), and each will be described.


6
a
b
c
d
1
2
3
4
5
start / Defense Evasion (TA0005) / Abuse Elevation Control Mechanism (T1548) / Setuid and Setgid (T1548.001)
Defense Evasion (TA0005)
+
Linux
macOS

Setuid and Setgid (T1548.001)

Description

An adversary may perform shell escapes or exploit vulnerabilities in an application with the setsuid or setgid bits to get code running in a different user's context. On Linux or macOS, when the setuid or setgid bits are set for an application, the application will run with the privileges of the owning user or group respectively. [1]. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn't need the elevated privileges.

Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications. These bits are indicated with an "s" instead of an "x" when viewing a file's attributes via `ls -l`. The `chmod` program can set these bits with via bitmasking, `chmod 4777 [file]` or via shorthand naming, `chmod u+s [file]`.

Adversaries can use this mechanism on their own malware to make sure they're able to execute in elevated contexts in the future.[2].

Platform(s): Linux macOS

1. **Technique Name (ID):** This is a link to MITRE ATT&CK that has the Technique name and ID.

2. **Tactic Selection:** Some Techniques (how the adversary did something) fit under multiple different Tactics (the goal of the adversary in their actions). This allows for selecting the Tactic to be used when adding this Technique to the cart in 3. The example Technique (T1566.002) only has a single Tactic – so this selection box will not be present in the actual app. It was added for documentation purposes. **NOTE:** If brought to this page from the search functions, you must select a tactic to use major functions of the page.

3. **Add to Cart:** This button adds a new cart entry that contains the Technique, it's Tactic, and a text box that can be used to provide the context behind the mapping. **NOTE:** If brought to this page from the search functions, you must select a tactic to add a technique to the cart.

4. **Description:** This describes the Technique. Reading this is useful in determining if a mapping should ultimately be made.

5. **Platform(s):** These are the OSes / systems in which this Technique could be used against. This is useful to check if it hadn't been filtered for before – as the Technique may not fit the platform(s) you have observed as a target of the behavior.

6. **Crumb Bar:** This is a set of links denoting the answer card path you took to the current page.

   a. **Start:** Takes you to the main question page.

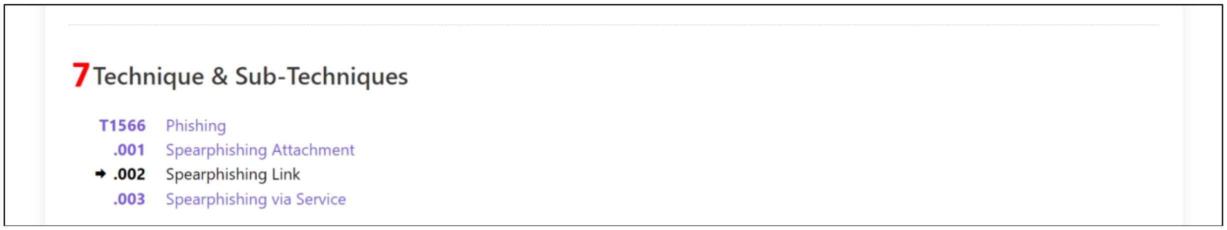
   b. **Tactic:** Links to the Tactic you're under.

   c. **Technique:** Links to the Technique you're under.

d. Sub-Technique: Links to the current Sub-Technique page displayed.

NOTE: If you're viewing a success page for a Technique that isn't a sub-technique, then this crumb will not exist – and the prior crumb will be the current page displayed.

The right-most crumb is the current page, and all crumbs to the left are considered the content parents of it. The current crumb is always unclickable – as you're already on that page.

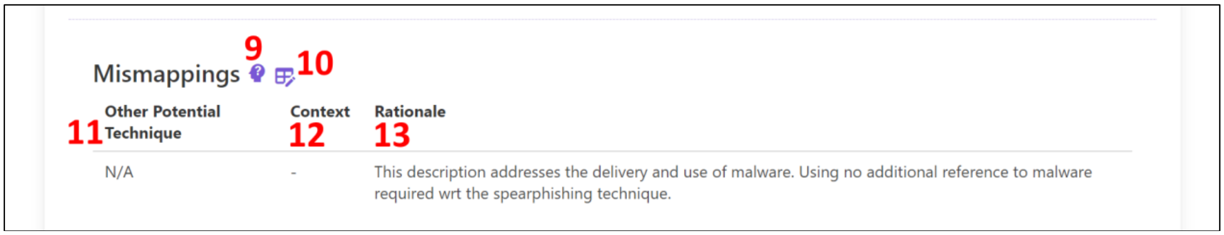


Technique & Sub-Techniques

T1566	Phishing
.001	Spearphishing Attachment
➡ .002	Spearphishing Link
.003	Spearphishing via Service

7. Technique/Sub-Technique Selector: Allows you to quickly jump between a Technique and its Sub-Techniques.

***8. Technique AKAs:** NOTE – AKAs have been removed from Decider.*



Mismappings

Other Potential Technique	Context	Rationale
N/A	-	This description addresses the delivery and use of malware. Using no additional reference to malware required wrt the spearphishing technique.

9. Tooltip: A mouse-over tooltip that provides an in-app documentation about mismappings.

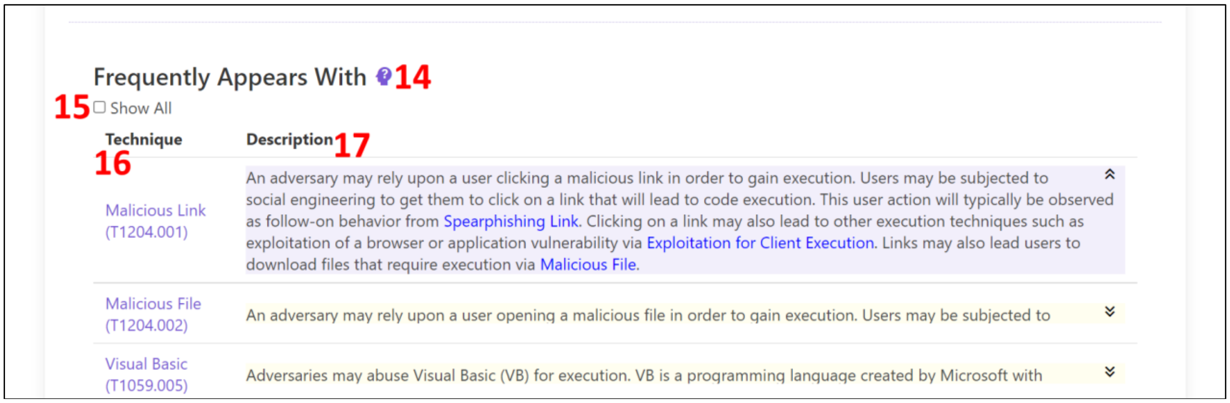
10. Edit Mis-mappings: This button opens the *Technique Mis-mappings Edit Page* for the Technique you're currently on. Such page allows for creating new mis-mappings, editing current ones, or removing them.

NOTE: If brought to this page from the search functions, you must select a tactic before navigating to the mismapping edit page.

11. Potential Technique: These are either *N/A* or in-app links to the correct Techniques. Each row describes an instance when the current Technique (the Technique page you're on) was an incorrect mapping and provides an alternative that was correct in that given scenario. When this is *N/A* – it means that the original mapping was incorrect, and that there is no correct mapping for the behavior.

12. Context: Provides background from the original source report that led to the Technique being mapped in that instance.

13. Rationale: This is a description as to why the original Technique (the current Technique page you're on) was not a correct mapping at the time, and why the other Technique mentioned was correct.



Frequently Appears With

□ Show All

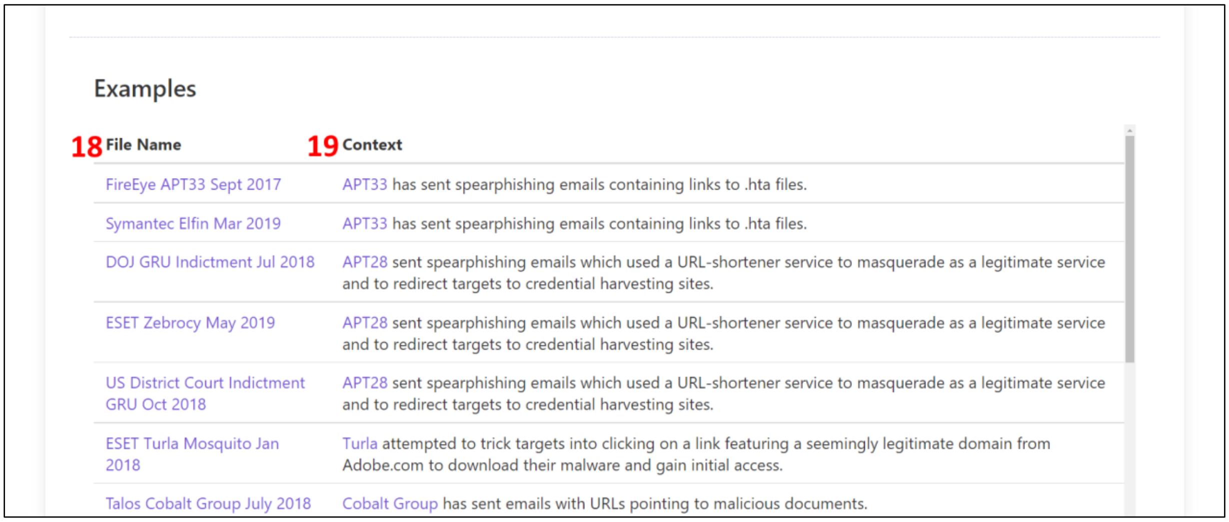
Technique	Description
Malicious Link (T1204.001)	An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Link. Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via Exploitation for Client Execution. Links may also lead users to download files that require execution via Malicious File.
Malicious File (T1204.002)	An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to
Visual Basic (T1059.005)	Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with

14. Tooltip: A mouse-over tooltip that provides an in-app documentation reference/background.

15. Show All Checkbox: Currently, only a sub-set of all entries are shown – this is to prevent bias in the suggestions given. When this is checked – all entries will be listed.

16. Technique: These are in-app links to the suggested Techniques. If the Technique you're currently on is correct – then these are suggestions of Techniques that typically appear with that Technique.

17. Description: These are the descriptions of the suggested Techniques. This allows quickly reading through what each Technique entails. As pictured, these start off as a single line and can be expanded by clicking them.



Examples

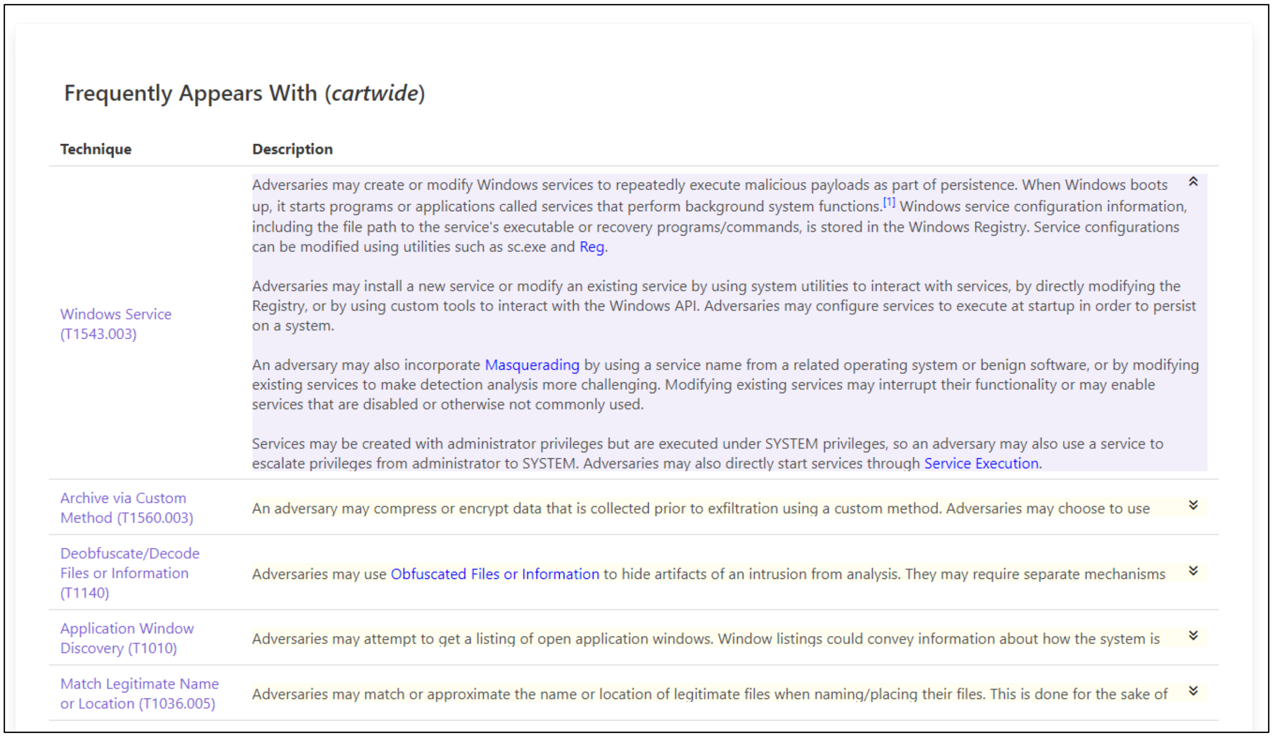
File Name	Context
FireEye APT33 Sept 2017	APT33 has sent spearphishing emails containing links to .hta files.
Symantec Elfin Mar 2019	APT33 has sent spearphishing emails containing links to .hta files.
DOJ GRU Indictment Jul 2018	APT28 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites.
ESET Zebrocy May 2019	APT28 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites.
US District Court Indictment GRU Oct 2018	APT28 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites.
ESET Turla Mosquito Jan 2018	Turla attempted to trick targets into clicking on a link featuring a seemingly legitimate domain from Adobe.com to download their malware and gain initial access.
Talos Cobalt Group July 2018	Cobalt Group has sent emails with URLs pointing to malicious documents.

18. File/Report Name: The document / report in which this Technique occurred.

19. Context: The actions taken by the adversary that led to the mapping of this Technique in the report.

Frequently Appears With *(cart-wide)*

This page functions similarly to the **Frequently Appears With** section as outlined in *Technique (Success) Page*. This page contains all suggested Techniques to map for all mapped Techniques already in the cart. The benefit is that there is a single place to access suggested Techniques to map – this is in contrast to manually going through the suggested Techniques for each entry in the cart.

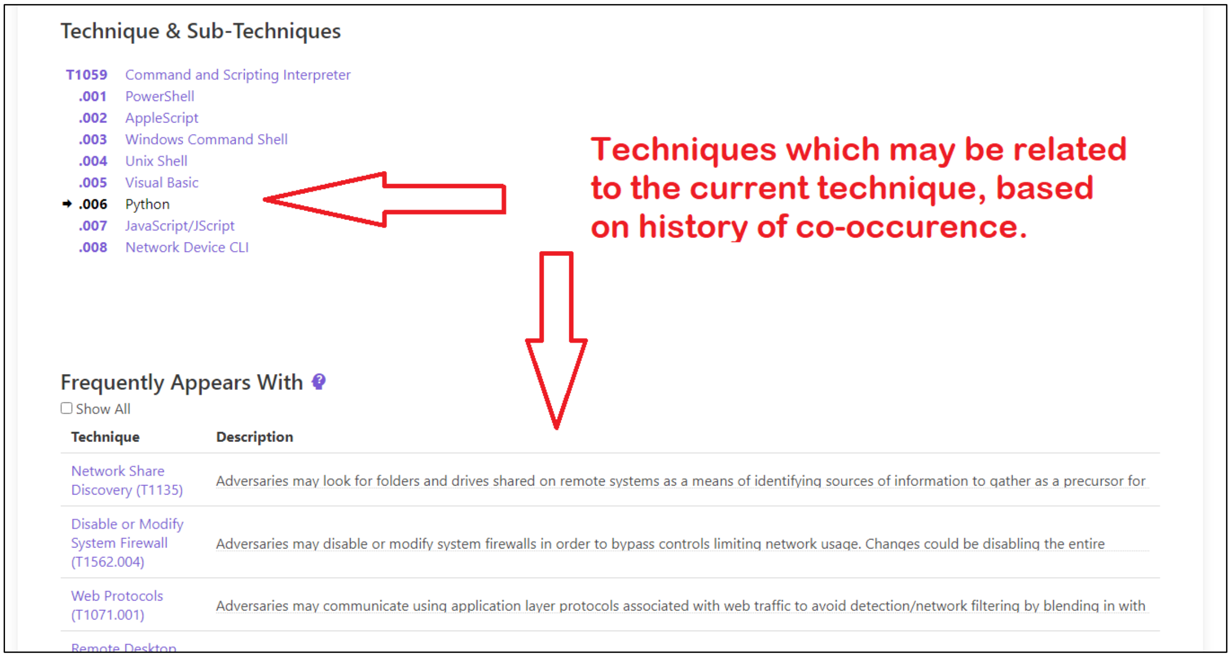


Frequently Appears With (*cartwide*)

Technique	Description
Windows Service (T1543.003)	Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions.[1] Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry. Service configurations can be modified using utilities such as sc.exe and Reg. Adversaries may install a new service or modify an existing service by using system utilities to interact with services, by directly modifying the Registry, or by using custom tools to interact with the Windows API. Adversaries may configure services to execute at startup in order to persist on a system. An adversary may also incorporate Masquerading by using a service name from a related operating system or benign software, or by modifying existing services to make detection analysis more challenging. Modifying existing services may interrupt their functionality or may enable services that are disabled or otherwise not commonly used. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through Service Execution.
Archive via Custom Method (T1560.003)	An adversary may compress or encrypt data that is collected prior to exfiltration using a custom method. Adversaries may choose to use
Deobfuscate/Decode Files or Information (T1140)	Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms
Application Window Discovery (T1010)	Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is
Match Legitimate Name or Location (T1036.005)	Adversaries may match or approximate the name or location of legitimate files when naming/placing their files. This is done for the sake of

“Frequently Appears With” (also known as Technique Co-occurrence)

When analyzing the threat reports mapped in ATT&CK itself, we have found certain technique pairs occur more commonly in threat reports than others. This **co-occurrence** can be scored, and we then use this information to identify potentially “related” techniques to display for the analyst.



Technique & Sub-Techniques

T1059	Command and Scripting Interpreter
.001	PowerShell
.002	AppleScript
.003	Windows Command Shell
.004	Unix Shell
.005	Visual Basic
➜ .006	Python
.007	JavaScript/JScript
.008	Network Device CLI

Techniques which may be related to the current technique, based on history of co-occurence.

Frequently Appears With

☐ Show All

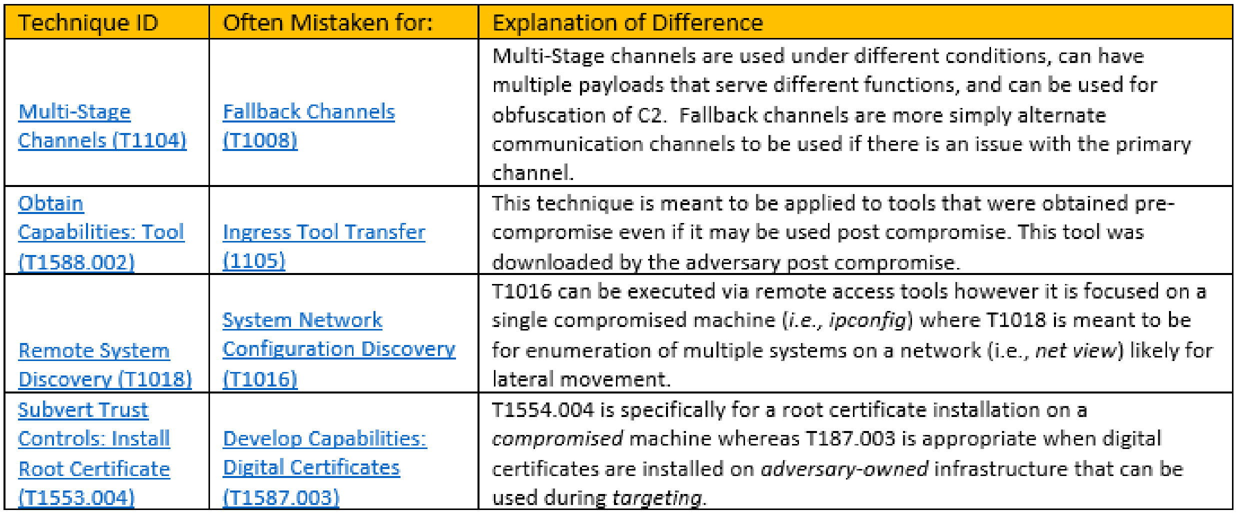
Technique	Description
Network Share Discovery (T1135)	Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for
Disable or Modify System Firewall (T1562.004)	Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage. Changes could be disabling the entire
Web Protocols (T1071.001)	Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with
Remote Desktop	

In the Decider application, the initial view is a randomized list of the techniques that more commonly co-occur with the current technique. These are randomized (versus, for example, listing them by number or alphabetically) to avoid potential bias. To display the full list, simply select the check box.

Note: co-occurrences do not guarantee that those techniques were used by the adversary. It simply indicates potential - something for an analyst to consider looking at, if it relates to the threat report they are reviewing.

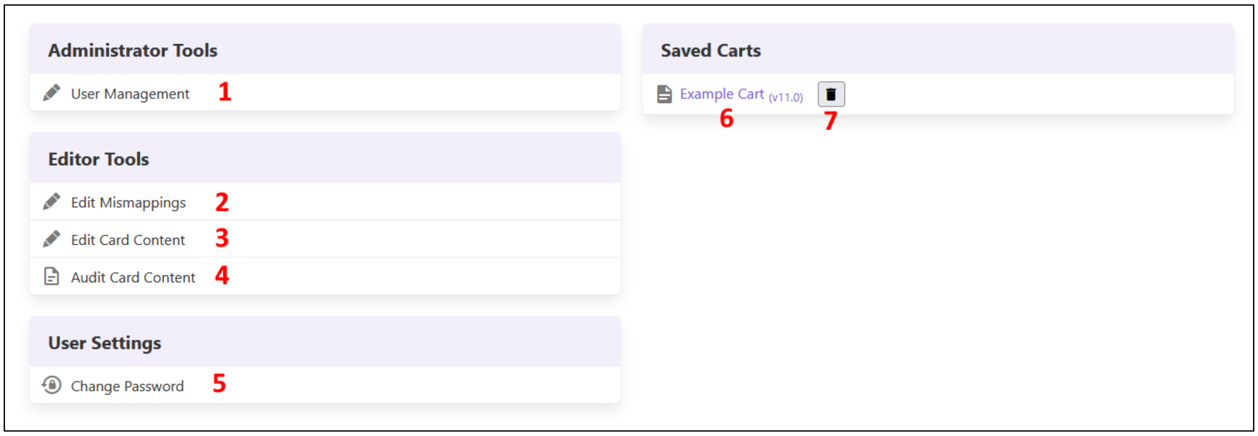
Mismappings

Mismappings can occur when an adversary behavior is incorrectly mapped to a technique or sub-technique. This often happens when the adversary activity occurs in a different phase of the attack lifecycle (or tactic) than reflected in the mapping or when the mapping incorrectly identifies the specific adversary behavior. Since many of the technique and sub-techniques have subtle differences, mis-mappings are bound to occur. This feature allows analysts to understand previously mis-mapped techniques as well as the proposed correction or alternative techniques. CISA analyst can use the mis-mappings as a guide and mechanism to build their own knowledge base of mis-mappings should they chose to do so while also aiding in simplifying and decreasing common oversights of mis-mapping techniques.



Technique ID	Often Mistaken for:	Explanation of Difference
Multi-Stage Channels (T1104)	Fallback Channels (T1008)	Multi-Stage channels are used under different conditions, can have multiple payloads that serve different functions, and can be used for obfuscation of C2. Fallback channels are more simply alternate communication channels to be used if there is an issue with the primary channel.
Obtain Capabilities: Tool (T1588.002)	Ingress Tool Transfer (1105)	This technique is meant to be applied to tools that were obtained pre-compromise even if it may be used post compromise. This tool was downloaded by the adversary post compromise.
Remote System Discovery (T1018)	System Network Configuration Discovery (T1016)	T1016 can be executed via remote access tools however it is focused on a single compromised machine (*i.e., ipconfig*) where T1018 is meant to be for enumeration of multiple systems on a network (i.e., *net view*) likely for lateral movement.
Subvert Trust Controls: Install Root Certificate (T1553.004)	Develop Capabilities: Digital Certificates (T1587.003)	T1554.004 is specifically for a root certificate installation on a *compromised* machine whereas T187.003 is appropriate when digital certificates are installed on *adversary-owned* infrastructure that can be used during *targeting*.

Profile



The profile page, accessible at '/profile' when logged-in, allows the use of Decider functions related to account information maintenance, access to previously saved carts, as well as editing and administrative tools (*depending on the current user's role*). The screenshot above displays the profile tab of an authenticated user with 'Admin' and 'Editor' privileges enabled. A user with only 'Member' permissions will not see items 1, 2, 3, and 4 and cannot access these routes.

1. **User Management:** Add, edit, or remove users from Decider. See Administrator Tools – User Management for more information.

2. **Edit Mismappings:** Edit the mismappings that appear on each respective technique/sub-technique success page. See Editor Tools – Edit Mismappings for more information.

3. **Edit Card Content:** Edit the question content of Decider, including tactic, technique, and sub technique questions / answers. See Editor Tools – Edit Card Content for more information.

4. **Audit Card Content:** Generates a table of missing question / answer card content. This table also mentions any cards that have style issues (i.e., bolding, punctuation, etc). See Editor Tools – Audit Card Content for more information.

5. **Change Password:** Allows any logged-in user to change their password. Clicking this brings the user to a page where they enter their new password.

6. **Load Cart:** Loads a previously saved cart from the 'Save Cart to Database' function. All previously saved carts will populate here. Clicking on a link here will unload/delete the current cart and replace it with the cart chosen.

7. **Delete Cart:** Deletes the cart. Each cart will have its respective delete button.

NOTE: Admin / editing features are outlined in the admin guide as a typical user will not need them.