Centro de
Investigación en
Computación

MITRE ATT&CK

Framework de Ataque

Definitions

Research

Course

Análisis y Detección de Malware

Instructor

Acosta Bermejo Raúl

Lecture notes

2024-B
23 de octubre del 2024

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Explicación del framework
3. Casos de Uso
4. Herramientas
5. Conclusiones

Introducción

Intro

Ciclos de Vida del Adversario

1. Cyber Kill Chain
2. NIST CyberSecurity Framework (CSF)
   i. El NIST ha creado varios frameworks y se recomienda usarlos en combinación según las necesidades.
      NIST Privacy Framework.
      Risk Management Framework (RMF)
   ii. Definhttps://www.nist.gov/cyberframework
3. MITRE ATT&CK

Introducción

Usos

Estos *frameworks* ofrecen:

1. Una taxonomía común que unifica términos y métodos.
2. Presentan un punto de vista del atacante.

   ¿Se debe pensar como Criminal para resolver casos?
3. Permite integrar CIT (*Cyber Threat Intelligence*) para relacionar distintos grupos conocidos como APT (*Advanced Persisten Threat*).

MITRE ATT&CK

Framework

MITRE ATT&CK

Introducción

- El MITRE es un centro de investigación y desarrollo con financiamiento federal de EU. Fundado en 1958 (65 años) actualmente tiene 42 centros.
- ATT&CK.
  - **A**dversarial **T**actics **T**echniques & **C**ommon **K**nowledge
  - Es una base de conocimiento de tácticas de adversario y técnicas, todas obtenidas de observaciones del mundo real.
- Estructura de la base
  - Tres tipos de modelo (matrices):

    Enterprise, Movile, ICS (*Industrial Control Systems,* Ej. SCADA).
  - Tres elementos en cada matriz

    TTP = **T**ácticas + **T**écnicas (sub-tec) + **P**rocedimientos

    Objetivo Como
- URL
  - https://mitre.org/
  - https://attack.mitre.org/

MITRE ATT&CK

Introducción

Las matrices están muy completas y se revisan y actualizan periódicamente.

Matriz	Tácticas	Técnicas	Otros elementos
Enterprise	14	235 435 Sub-técnicas	Software: 794 Data sources: 37 Mitigations: 43 Assets: 14 Grups: 152 Campaigns: 28
Mobile	12	86	
ICS	12	94	

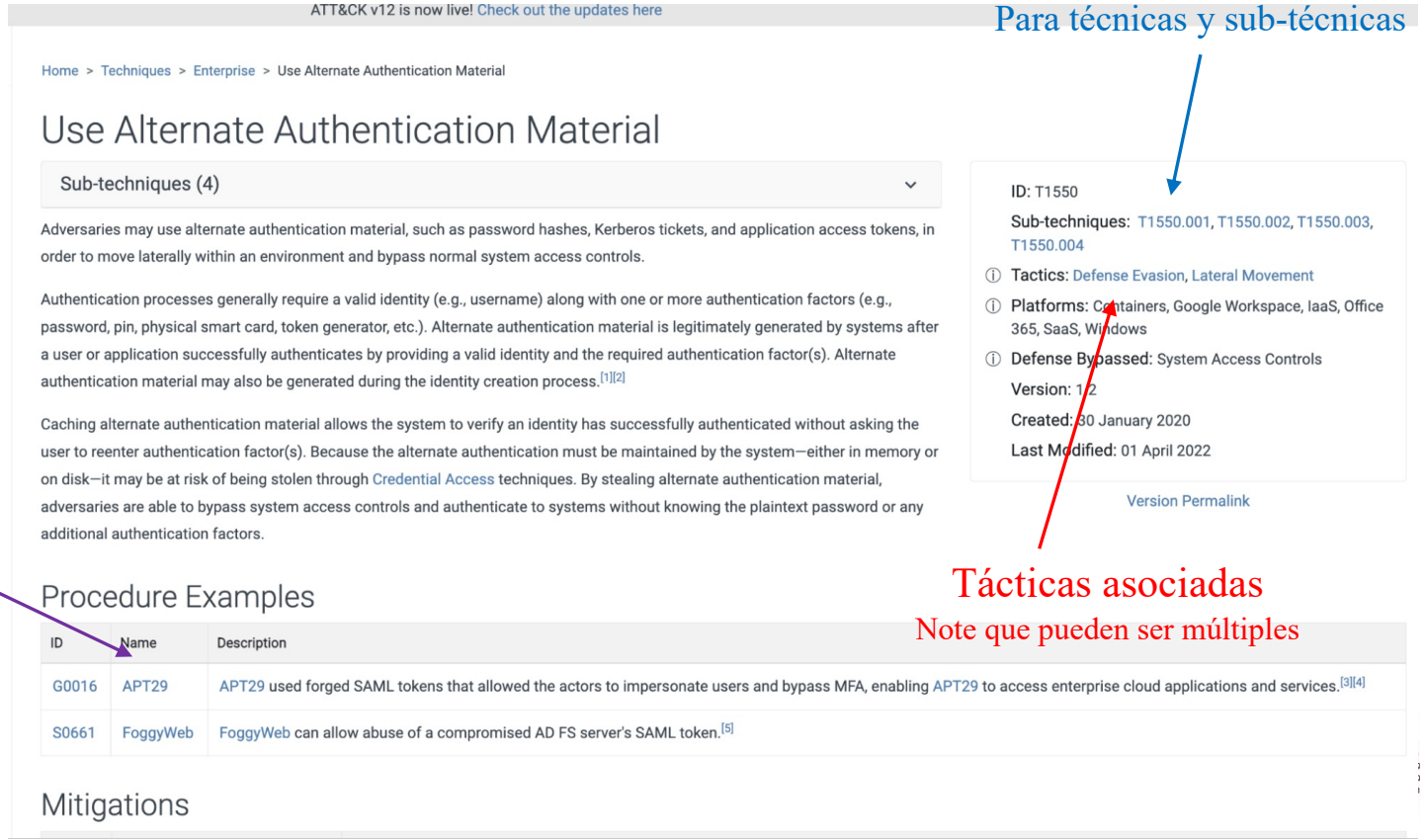
Cada técnica incluye:

1. Una descripción de la técnica.
2. Una o varias sub-técnicas relacionadas.
3. Tácticas de mitigación.
4. Tácticas de detección.
5. Metadatos relacionados para propósitos de indexación.
6. Referencias a incidentes reales.

MITRE ATT&CK

Introducción

Ejemplo de **Técnica**



Identificadores
Para técnicas y sub-técnicas

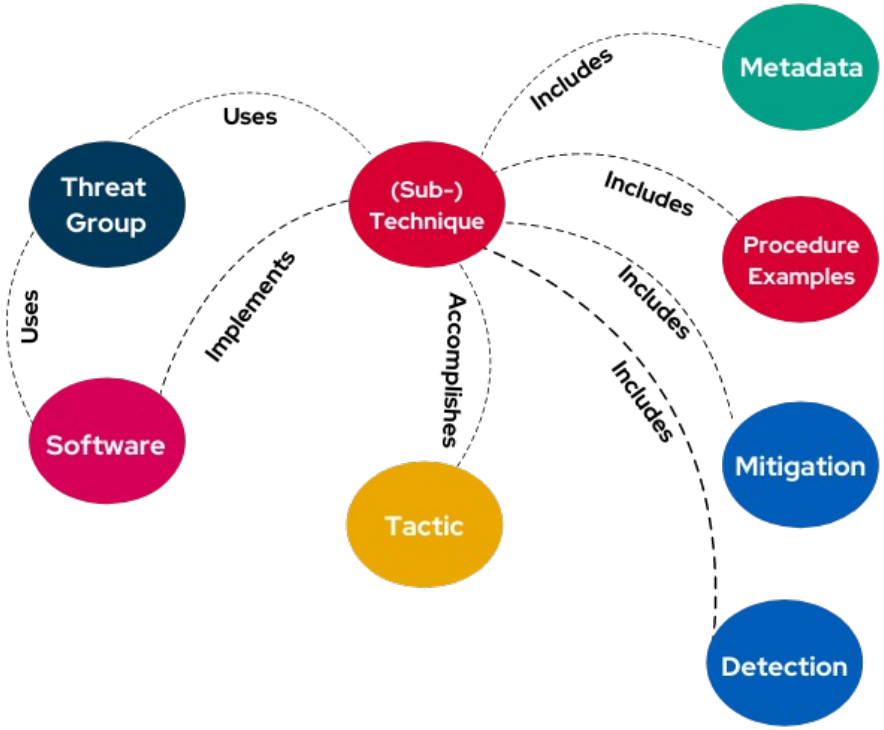
Procedimientos
Son descripciones de incidentes reales

Tácticas asociadas
Note que pueden ser múltiples

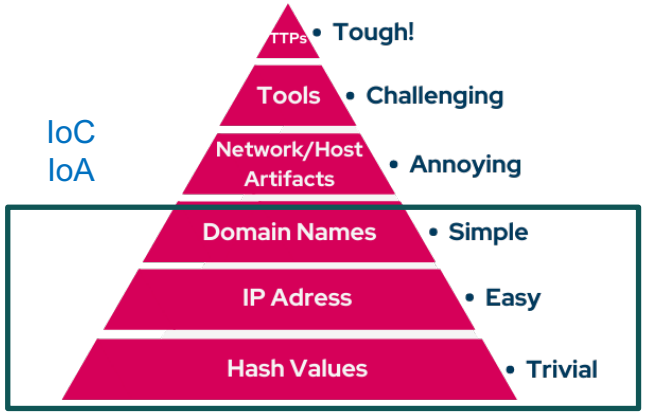
MITRE ATT&CK

Introducción

Fuente: https://www.picussecurity.com/mitre-attack-framework-beginners-guide



The Pyramid of Pain (David Bianco, 2013)



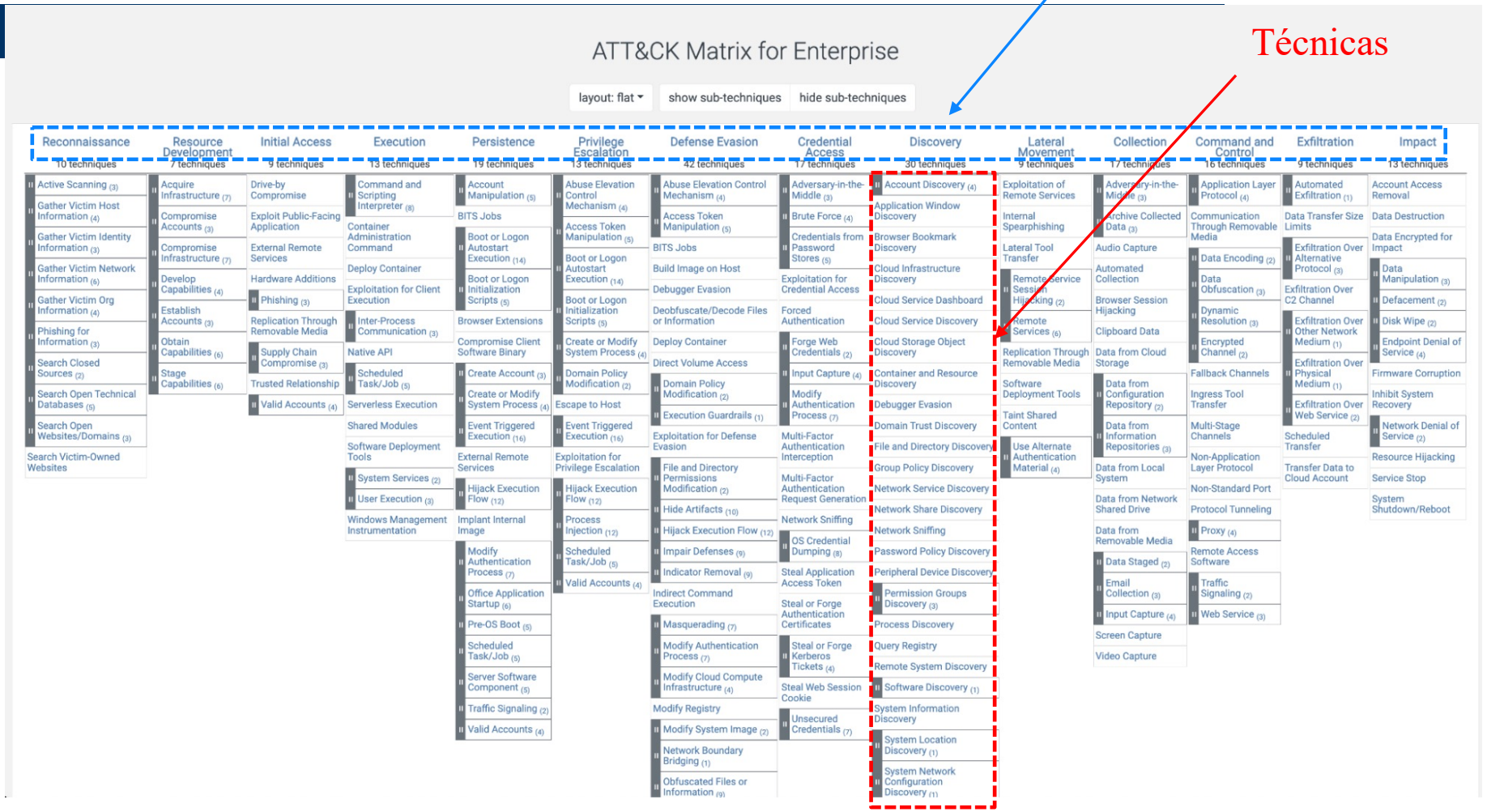
IoC (*Indicators of Compromise*) **Violación**
IoA (*Indicators of Attack*) Sospecha

MITRE ATT&CK

Ejemplo de matriz

Tácticas

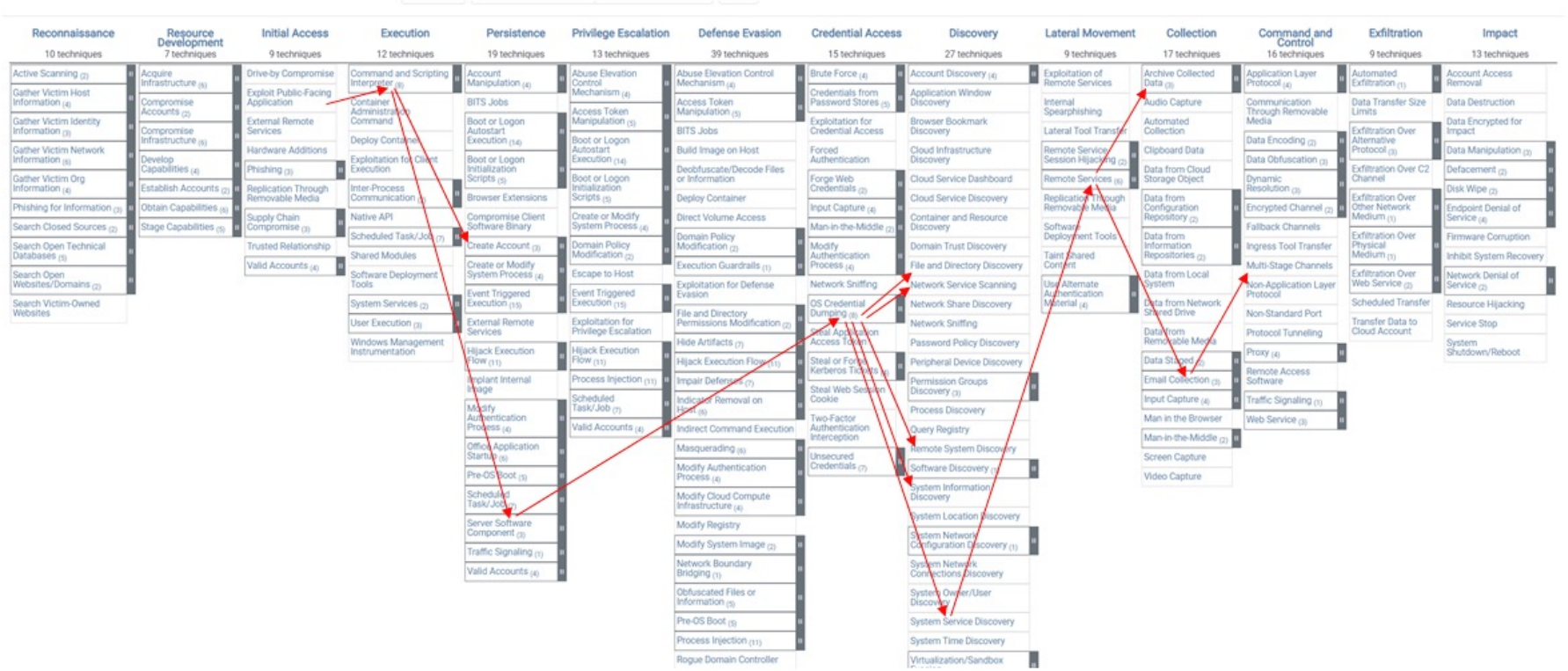
Técnicas



MITRE ATT&CK

Intro

Un **Vector de Ataque** es la ejecución de múltiples TTPs realizados tanto en secuencia como en paralelo.



MITRE ATT&CK

Introducción

Cada matriz tiene subdominios de especialización que la hacen de aplicación específica:

1. Enterprise
   - **i. PRE**
   - ii. Windows
   - iii. macOS
   - iv. Linux
   - v. Cloud
2. i. Mobile
   - i. Android
   - ii. iOS
3. ii. ICS
   - i. No tiene

Como PREpararse para un ataque

No es un estándar estático y periódicamente saca nuevas versiones que pueden agregar nuevas técnicas

La versión actual es:
V15.1
23 de abril de 2024

MITRE ATT&CK

Introducción

Id.	G0018.
Name	admin@338
Desc.	It is a China-based cyber threat group

Otros elementos

Grupos

- Son grupos de actividades que son rastreadas con un nombre en común.
- Los analistas rastrean estos grupos utilizando diversas metodologías analíticas y términos como grupos de amenazas, grupos de actividades y actores de amenazas.
- Algunos grupos tienen varios nombres asociados con actividades similares debido a que varias organizaciones rastrean actividades similares con diferentes nombres.
- Las definiciones de grupos de las organizaciones pueden superponerse parcialmente con los grupos designados por otras organizaciones y pueden diferir en una actividad específica.

MITRE ATT&CK

Introducción

Otros elementos

Campañas

- La comunidad de seguridad rastrea actividades de intrusión usando varias metodologías analíticas y términos tales como operaciones, conjunto de intrusiones, y campañas.
- Para el equipo de MITRE ATT&CK utiliza el término Campaña para describir cualquier agrupación de actividades de intrusión realizadas durante un período de tiempo específico con objetivos y metas comunes.

Id.	C0034
Grupos asociados:	G0034
Desc.	2022 Ukraine Electric Power Attack
Documento (82 pag.)	https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Casos de Uso

Como usar el framework

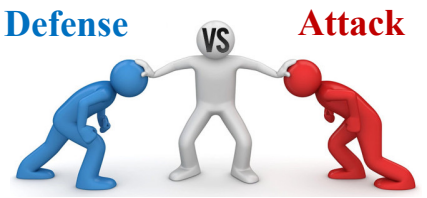
Ejemplos

Casos de Uso

Intro

El MITRE ATT&CK se puede usar de varias formas y la siguiente lista enuncia las más comunes:

- Defensa
  1. Para realizar un Análisis de la Seguridad
     1. Gestión de riesgos, *Hunting Threats*, etc.
  2. Para mejorar las defensas
     - Construir una plataforma defensiva.
  3. Para entrenar a un equipo **Blue**
     - Respuesta a incidentes
- Ataque
  1. Para emular a un adversario.
  2. Para entrenar a un equipo **Rojo**
     - *Pentesting* / Hackeo ético



Casos de Uso

Intro

El MITRE ATT&CK se puede usar de varias formas y la siguiente lista enuncia las más comunes:

Tools

Herramientas

Software

Tools

Software

Las más conocidas

1. Navigator
   - *It is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more*.
   - URL: https://mitre-attack.github.io/attack-navigator/
     https://github.com/mitre-attack/attack-navigator
2. Caldera
   - *A Scalable, Automated Adversary Emulation Platform*.
   - URL: https://caldera.mitre.org/
     https://caldera.readthedocs.io/en/latest/
3. STIX
   - Formato de intercambio de datos de ataque.

Tools

Software

Otras URLs

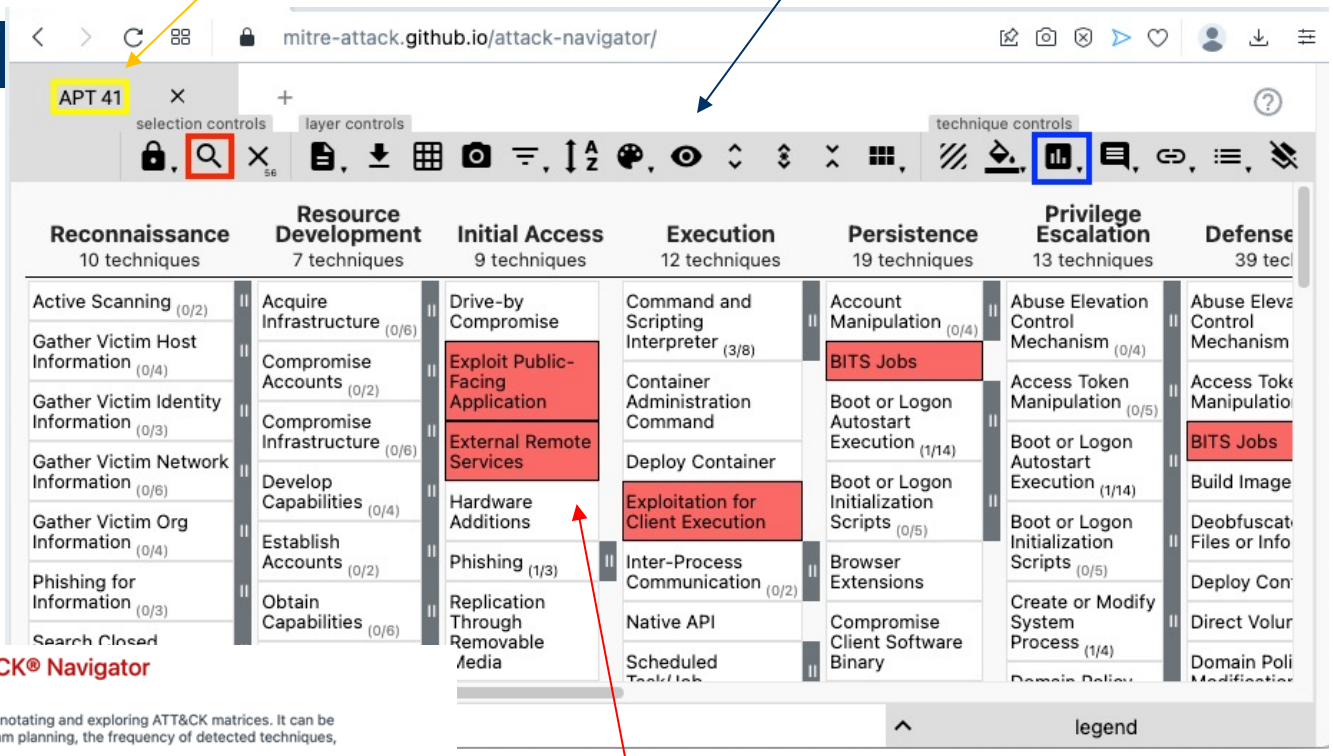
- https://samsclass.info/152/proj/attack_nav.htm

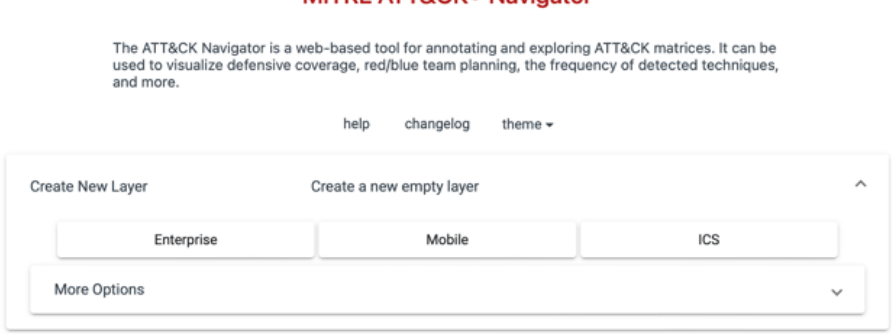
Layer
con nombre asignado

Controles
barra

Navigator

- Trabaja con capas (layers).
- Cada capa puede especificar un dominio tecnológico específico: matriz, sistema operativo, etc.





Selección
Tácticas y Técnicas

Tools

Software

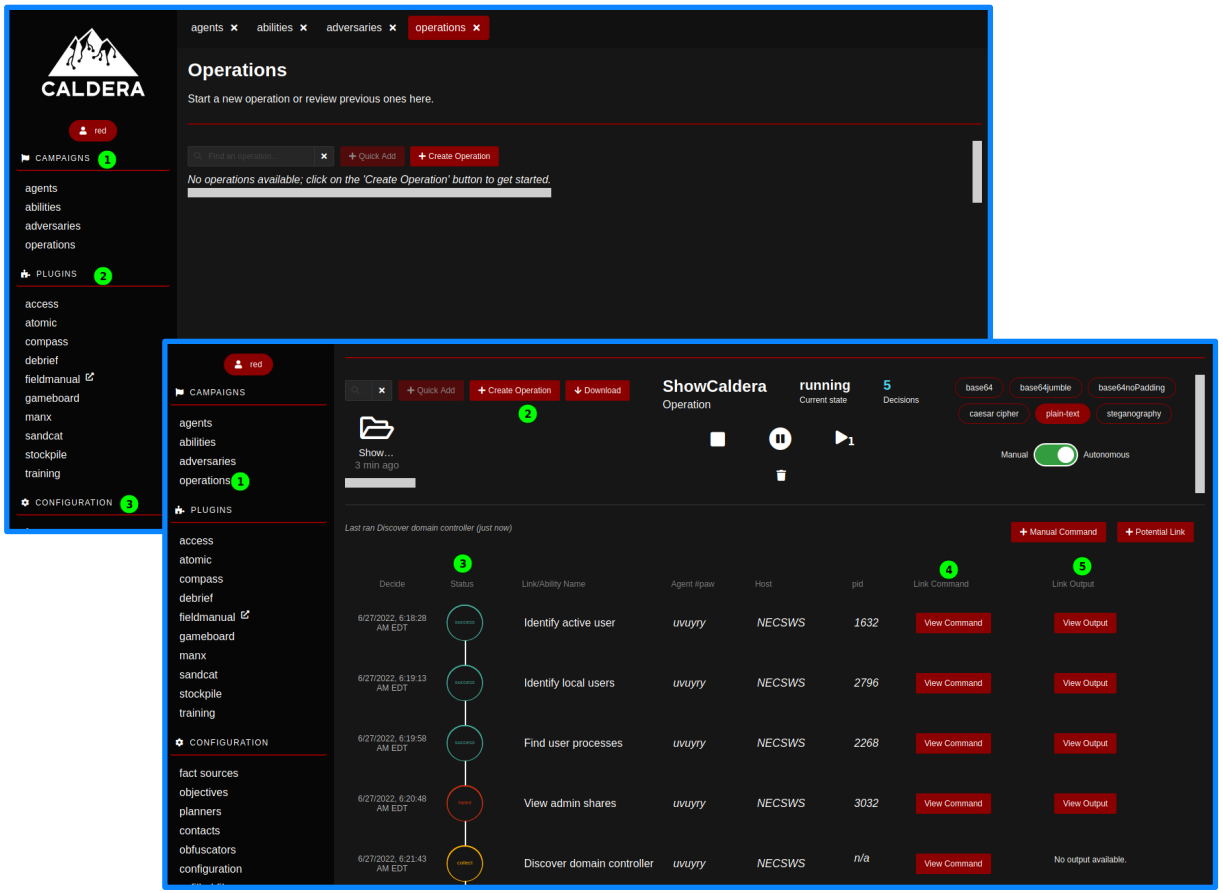
Otras URLs

- https://natasec.com/mitre-caldera-primeros-pasos/
- https://cylab.be/blog/226/mitre-attck-in-practice-part-ii-caldera

Caldera

Está formado por:

1. Servidor:
   Web App + API rest.
2. Agentes.



Tools

Software

También se puede descargar la información en **Excel**.
https://attack.mitre.org/resources/attack-data-and-tools/

STIX

Información oficial del sitio:

1. *Structured Threat Information Expression* (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). **JSON**
2. The ATT&CK dataset is available in STIX 2.0 and STIX 2.1.
3. Other presentations of this dataset, including the ATT&CK Navigator and this website, are built from the STIX data.
4. TAXII
    i. The ATT&CK STIX data can also be accessed via the official ATT&CK TAXII™ server.
    ii. *Trusted Automated Exchange of Intelligence Information* (TAXII) is an application protocol for exchanging CTI over HTTPS.
    iii. The ATT&CK TAXII server provides API access to the ATT&CK STIX knowledge base.

Tools

Software

Otro tipo de herramientas

- Existen muchas herramientas comerciales y algunas gratuitas que basan su funcionamiento den el MITRE ATT&CK.
  - CrowdStrike: Falcon (EDR, *Endpoint Detection and Response*)
- Estas herramientas siempre inician con una idea/concepto clave que se prueba con un prototipo.
- Estas herramientas se pueden desarrollar a nivel Licenciatura o Posgrado.
  - *Automated generation of attack trees based on MITRE ATT&CK*
  - Trabajo Terminal de ESCOM, Andrés Nieves.
  - 24 de septiembre de 2024, https://ccc.inaoep.mx/~cisma/

Conclusions

Conclusiones

Resumen

Conclusiones

Generales

El *framework* del MITRE ATT&CK es bueno para:

- Comprender todos los tipos de ataque de manera general (vector, fases y secuencia de pasos) así como de forma específica (procedimientos concretos).

Sin embargo, en Ciberseguridad siempre hay que complementar el trabajo con:

- Otros frameworks: CAPEC, CWE, CIS controls, etc.
- Otras herramientas
- Estandares, guias, manuales, etc. Mejores prácticas
  - NIST, SANS, ISO 27mil, etc.

Conclusiones

Generales

Por quinta ocasión se realizará el

MITRE ATT&CKcon 5.0

October 22,23, 2024 at 6:55 AM CST

La asistencia es física (con costo) y virtual (gratuita).

- https://mitre.brandlive.com/ATTACKCon-5-0/en/home
- AGENDA: https://na.eventscloud.com/website/76470/

The end

Contacto

Raúl Acosta Bermejo

http://www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/
https://www.cic.ipn.mx/~racostab/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652