



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





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. Definir <https://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 Persistent 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, Mobile, 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

Procedimientos
Son descripciones
de incidentes reales

ATT&CK v12 is now live! [Check out the updates here](#)

Home > Techniques > Enterprise > Use Alternate Authentication Material

Use Alternate Authentication Material

Sub-techniques (4)

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process.^{[1][2]}

Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](#) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

Procedure Examples

ID	Name	Description
G0016	APT29	APT29 used forged SAML tokens that allowed the actors to impersonate users and bypass MFA, enabling APT29 to access enterprise cloud applications and services. ^{[3][4]}
S0661	FoggyWeb	FoggyWeb can allow abuse of a compromised AD FS server's SAML token. ^[5]

Mitigations

Identificadores
Para técnicas y sub-técnicas

ID: T1550
Sub-techniques: T1550.001, T1550.002, T1550.003, T1550.004
① Tactics: Defense Evasion, Lateral Movement
① Platforms: Containers, Google Workspace, IaaS, Office 365, SaaS, Windows
① Defense Bypassed: System Access Controls
Version: 1.2
Created: 30 January 2020
Last Modified: 01 April 2022
[Version Permalink](#)

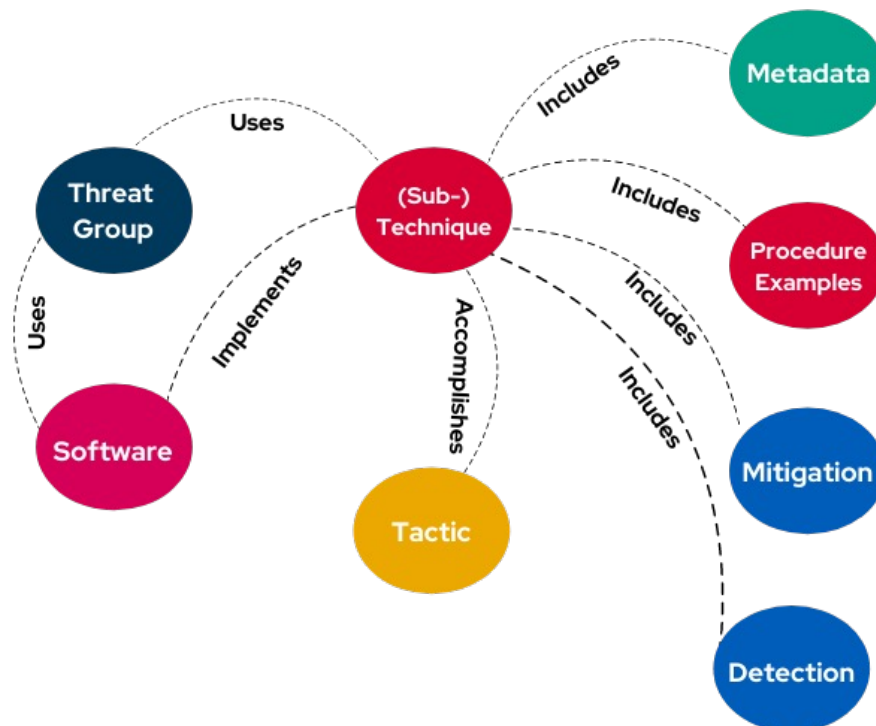
Tácticas asociadas
Note que pueden ser múltiples



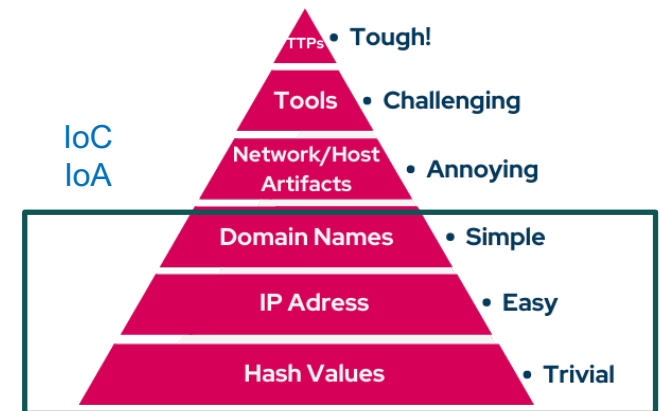
MITRE ATT&CK

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

ATT&CK Matrix for Enterprise

layout: flat ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Infrastructure (7) Compromise Accounts (3) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (6) Stage Capabilities (6)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Command and Scripting Interpreter (8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (5) Serverless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (5) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Domain Policy Modification (2) Escape to Host Event Triggered Execution (16) External Remote Services Hijack Execution Flow (12) Implant Internal Image Modify Authentication Process (7) Office Application Startup (6) Pre-OS Boot (5) Scheduled Task/Job (5) Server Software Component (5) Traffic Signaling (2) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) File and Directory Permissions Modification (2) Hide Artifacts (16) Hijack Execution Flow (12) Impair Defenses (9) Indicator Removal (9) Indirect Command Execution Masquerading (7) Modify Authentication Process (7) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (9)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) File and Directory Permissions Modification (2) Hide Artifacts (16) Hijack Execution Flow (12) Impair Defenses (9) Indicator Removal (9) Indirect Command Execution Masquerading (7) Modify Authentication Process (7) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (9)	Adversary-in-the-Middle (3) Brute Force (4) Credentials from Password Stores (5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (7) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Authentication Certificates Steal Web Session Cookie Unsecured Credentials (7)	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (3) Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Location Discovery (1) System Network Configuration Discovery (1)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (3) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Remote Access Software Traffic Signaling (2) Web Service (3)	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (2) Scheduled Transfer Transfer Data to Cloud Account Transfer Data to Local System Proxy (4)	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot



MITRE ATT&CK

Intro

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

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (3) Gather Victim Org Information (4) Phishing for Information (5) Search Closed Sources (2) Search Open Technical Databases (3) Search Open Websites/Domains (2) Search Victim-Owned Websites	Acquire Infrastructure (8) Compromise Accounts (2) Compromise Infrastructure (8) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (3) Stage Capabilities (5)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Command and Scripting Interpreter (8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (7) Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (15) External Remote Services Hijack Execution Flow (11) Implant Internal Image Modify Authentication Process (4) Office Application Startup (8) Pre-OS Boot (3) Scheduled Task/Job (7) Server Software Component (3) Traffic Signaling (1) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (3) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (7) Impair Defenses (7) Indicator Removal on Host (4) Indirect Command Execution Masquerading (8) Modify Authentication Process (4) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (3) Pre-OS Boot (3) Process Injection (11) Rogue Domain Controller	Abuse Elevation Control Mechanism (4) Access Token Manipulation (3) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (7) Impair Defenses (7) Indicator Removal on Host (4) Indirect Command Execution Masquerading (8) Modify Authentication Process (4) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (3) Pre-OS Boot (3) Process Injection (11) Rogue Domain Controller	Brute Force (4) Credentials from Password Stores (3) Exploitation for Credential Access Forge Web Credentials (2) Input Capture (4) Man-in-the-Middle (3) Modify Authentication Process (4) Network Sniffing OS Credential Dumping (8) Remote Application Access (1) Steal or Forge Kerberos Tickets (4) Steal Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials (7)	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (3) Process Discovery Query Registry Remote System Discovery Software Discovery (3) System Information Discovery System Location Discovery System Network Configuration Discovery (1) System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (8) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Archive Collected Data (3) Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (2) Data from Information Repositories (2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Stored (2) Email Collection (3) Input Capture (4) Man in the Browser Man-in-the-Middle (2) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (1) Web Service (3)	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (3) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot



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
- i. Mobile
 - i. Android
 - ii. iOS
- 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

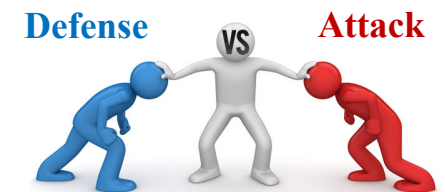
El MITRE ATT&CK se puede usar de varias formas y la siguiente lista enuncia las más comunes:

❖ 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.



Otras URLs

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



Tools

Software

Navigator

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

MITRE ATT&CK® Navigator

The ATT&CK Navigator 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.

help changelog theme

Create New Layer

Create a new empty layer

Enterprise

Mobile

ICS

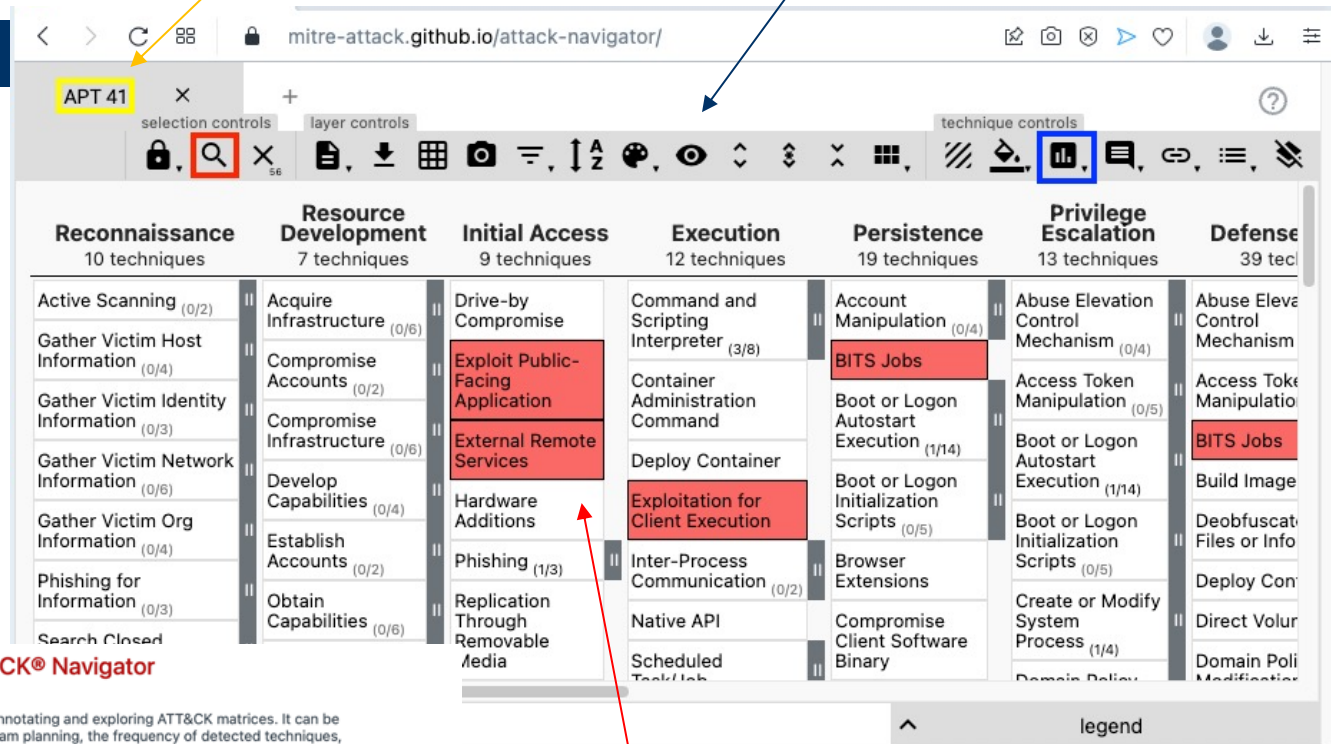
More Options

Layer

con nombre asignado

Controles

barra



Selección

Tácticas y Técnicas



Otras URLs

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



Tools

Software



Caldera

Está formado por:

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

Decide	Status	Link/Ability Name	Agent IP	Host	pid	Link Command	Link Output
6/27/2022, 6:18:28 AM EDT	Running	Identify active user	uvuyry	NECSWS	1632	View Command	View Output
6/27/2022, 6:19:13 AM EDT	Running	Identify local users	uvuyry	NECSWS	2796	View Command	View Output
6/27/2022, 6:19:58 AM EDT	Running	Find user processes	uvuyry	NECSWS	2268	View Command	View Output
6/27/2022, 6:20:48 AM EDT	Running	View admin shares	uvuyry	NECSWS	3032	View Command	View Output
6/27/2022, 6:21:43 AM EDT	Running	Discover domain controller	uvuyry	NECSWS	n/a	View Command	No output available.



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 en 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, guías, 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

