Matriz Mitre ATT&CK®
for Enterprise
V12

Tácticas, técnicas y conocimiento común de adversarios **(11/2022)**

/in/jordigasconprojects/

¿QUÉ ES MITRE ATT&CK?

Se trata de una base de conocimiento en el que se muestran las **tácticas y técnicas** que forman parte **del ciclo de vida de un ciberataque**.

Utilizada por los equipos Red Team (ofensivos) para modelar ataques, y equipos Blue Team (defensivo) para mitigaciones.

/in/jordigasconprojects/

TÉCNICAS ENTERPRISE

En la actualidad la matriz está conformada por **14 técnicas.**

ID	Nombre	Descripción
TA0043	Reconocimiento	El adversario está tratando de recopilar información que pueda usar para planificar operaciones futuras.
TA0042	Desarrollo de recursos	El adversario está tratando de establecer recursos que puedan usar para apoyar las operaciones.
TA0001	Acceso incial	El adversario está tratando de entrar en su red.

/in/jordigasconprojects/

TÉCNICAS ENTERPRISE

ID	Nombre	Descripción
TA0002	Ejecución	El adversario está tratando de ejecutar un código malicioso.
TA0003	Persistencia	El adversario está tratando de mantener su punto de apoyo.
TA0004	Elevación de privilegios	El adversario está tratando de obtener permisos de nivel superior.
TA0005	Evasión de defensa	El adversario está tratando de evitar ser detectado.

/in/jordigasconprojects/

TÉCNICAS ENTERPRISE

ID	Nombre	Descripción
TA0006	Acceso a credenciales	El adversario está tratando de robar nombres de cuenta y contraseñas.
TA0007	Descubrimiento	El adversario está tratando de averiguar su entorno.
TA0008	Movimiento lateral	El adversario está tratando de moverse a través de su entorno.
TA0009	Recopilación	El adversario está tratando de recopilar datos de interés para su objetivo.

/in/jordigasconprojects/

TÉCNICAS ENTERPRISE

ID	Nombre	Descripción
TA0011	Command & Control	El adversario está tratando de comunicarse con los sistemas comprometidos para controlarlos.
TA0010	Exfiltración	El adversario está tratando de robar datos.
TA0040	Impacto	El adversario está tratando de manipular, interrumpir o destruir sus sistemas y datos.

/in/jordigasconprojects/

TÁCTICAS ENTERPRISE

Cada una de las técnicas esta compuesta por una serie de **TÁCTICAS.**

ID	Nombre	Tácticas
TA0043	Reconocimiento	10
TA0042	Desarrollo de recursos	7
TA0001	Acceso incial	9
TA0002	Ejecución	13
TA0003	Persistencia	19

/in/jordigasconprojects/

TÁCTICAS ENTERPRISE

ID	Nombre	Tácticas
TA0004	Elevación de privilegios	13
TA0005	Evasión de defensa	42
TA0006	Acceso a credenciales	17
TA0007	Descubrimiento	30
TA0008	Movimiento lateral	9
TA0009	Recopilación	17

/in/jordigasconprojects/

TÁCTICAS ENTERPRISE

ID	Nombre	Tácticas
TA0011	Command & Control	16
TA0010	Exfiltración	9
TA0040	Impacto	13
	TOTAL	**224**

/in/jordigasconprojects/

FASES DEL CIBERATAQUE

PREPARACIÓN

- TA0043 Reconocimiento
- TA0042 Desarrollo de recursos

INTRUSIÓN

- TA0001 Acceso inicial
- TA0002 Ejecución
- TA0003 Persistencia

BRECHA ACTIVA

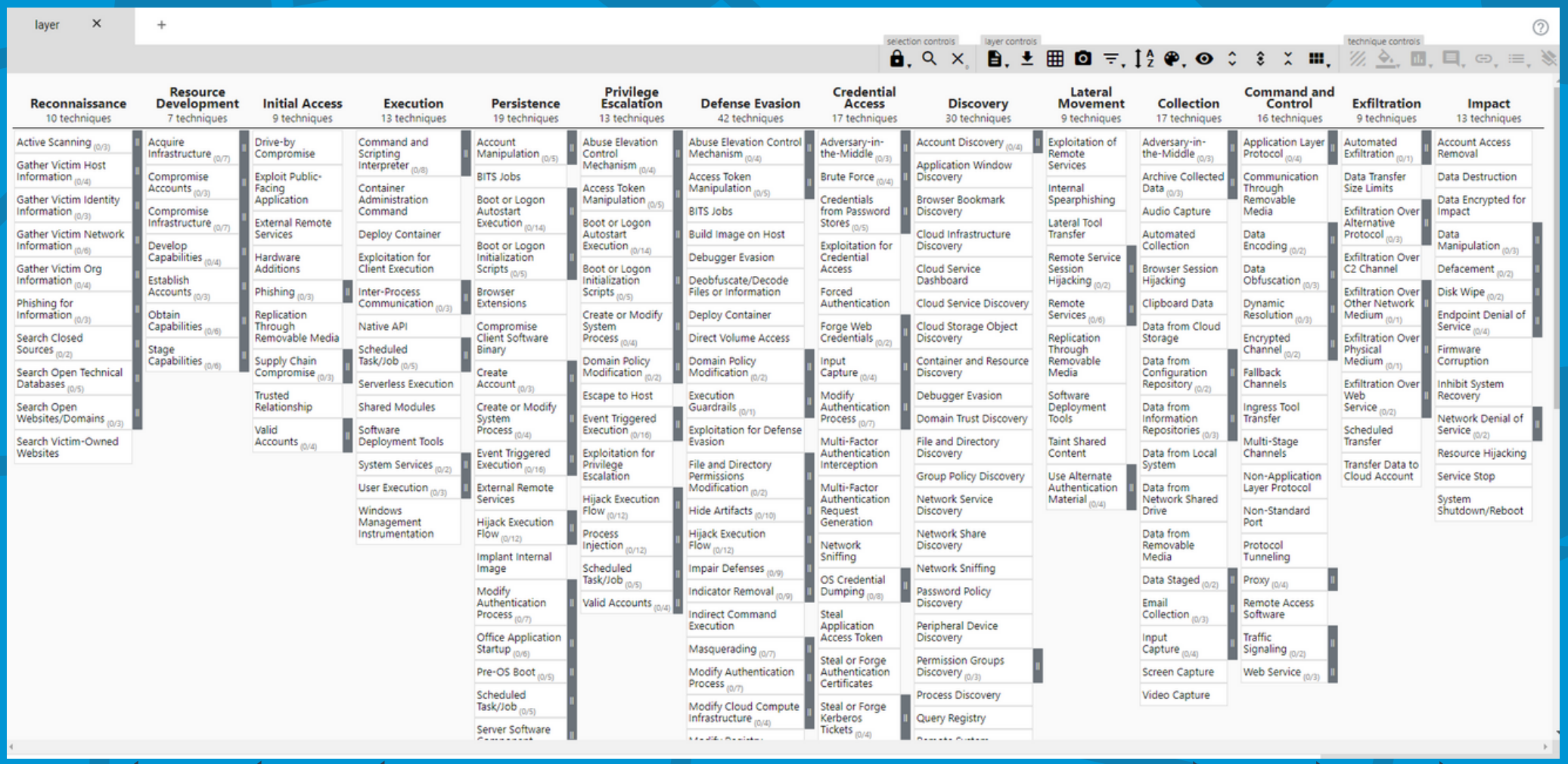
- TA0004 Escalada de privilegios
- TA0005 Evasión de defensas
- TA0006 Acceso a credenciales
- TA0007 Descubrimiento
- TA0008 Movimiento lateral
- TA0009 Recopilación
- TA0011 Command & Control
- TA0010 Exfiltración
- TA0040 Impacto

/in/jordigasconprojects/

Mitre ATT&CK Navigator

Disponible versión web totalmente **funcional y gratuita**.

https://mitre-attack.github.io/attack-navigator/



/in/jordigasconprojects/

¿PARA QUÉ USAR MITRE ATT&CK?

- Mapeo de controles defensivos
- Búsqueda de amenazas
- Actores de referencia (APT)
- Modelado de ataques (Red Team)

/in/jordigasconprojects/

ENLACES Y RECURSOS

Web oficial. Toda la información y acceso a los recursos disponibles de sus base de conocimiento

https://attack.mitre.org/

/in/jordigasconprojects/

ENLACES Y RECURSOS

MITRE ATT&CK Navigator. Aplicación web que nos permite el diseño de matrices personalizadas, exportación y otras posibilidades

https://mitre-attack.github.io/attack-navigator/

/in/jordigasconprojects/

Gracias por tu tiempo!

¿Conocías MITRE ATT&CK?

Comparte, comenta o etiqueta a quién pueda serle de interés

/in/jordigasconprojects/