Universidad Autónoma de Baja California

Facultad de Ciencias Químicas e Ingeniería

GESTIÓN Y SEGURIDAD EN REDES

Meta 3.1.1

MITRE ATT&CK

Docente: ALVAREZ SALGADO, CARLOS FRANCISCO

Alumno: Gómez Cárdenas, Emmanuel Alberto

Matricula: 01261509

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es un framework en la ciber-seguridad (desarrollado por MITRE Corporation) que cataloga tácticas y técnicas usadas por los adversarios en los ataques. Su importancia yace en proveer una estructura y un lenguaje para comprender, detectar y prevenir amenazas. En pocas palabras es un modelo que intenta categorizar sistemáticamente el comportamiento del adversario,

Este framework cubre una gama amplia de tácticas y técnicas utilizadas en diferentes etapas del ciclo de vida de un ciber-ataque, las cuales incluyen:

Tácticas

Objetivos generales buscados por los adversarios.

- **Reconocimiento:** recopilación de información para planificar el ataque.
- **Desarrollo de recursos:** establecimiento de recursos para apoyar las operaciones de ataque.
- **Acceso inicial:** penetrar en el sistema o red de destino.
- **Ejecución:** ejecución de malware o código malicioso en el sistema comprometido.
- **Persistencia:** mantener acceso al sistema comprometido.
- **Escalamiento de privilegios:** obtener acceso o permisos de nivel superior.
- **Evasión de defensa:** evitar la detección una vez dentro del sistema.
- **Acceso a credenciales:** robar nombres de usuario, contraseñas y otras credenciales de inicio de sesión.
- **Descubrimiento:** investigación del entorno de destino para saber a que recursos se puede acceder o controlar para respaldar un ataque planificado.
- **Movimiento lateral:** obtener acceso a recursos adicionales dentro del sistema.
- **Recopilación:** recopilación de datos relacionados con el objetivo del ataque.
- **Comando y control:** establecer comunicacionales encubiertas/indetectables que permitan al atacante controlar el sistema.
- **Exfiltración:** transferencia de datos fuera de la red comprometida.
- **Impacto:** interrumpir, dañar, deshabilitar o destruir datos o procesos de negocio.

Técnicas

Acciones específicas que los adversarios utilizan para lograr los objetivos generales definidos por las tácticas. Cada táctica en MITRE ATT&CK está asociada con una serie de técnicas específicas que describen cómo los adversarios intentan cumplir con esa táctica en particular.

Unos ejemplos para la táctica de reconocimiento seria:

- **Escaneo activo:** escanear activamente la red en busca de dispositivos y servicios vulnerables.
- **Reconocimiento pasivo:** recopilar información sobe el objetivo sin interactuar directamente con el.
- **Ingeniería social:** utilizar la manipulación psicológica para obtener información confidencial de los empleados de una organización.

En cuanto a escenarios prácticos esto puede ser utilizado para la detección de MALWARE, prevención de ataques de PHISING o para mitigar ataques de RANSOMWARE.

Conclusión:

MITRE ATT&CK es una herramienta muy poderosa en la seguridad cibernética ya que ayuda a entender, detectar y prevenir ataques, los cuales, si no son tratados acordemente pueden dañar la integridad de una organización.

Referencias:

BM. (s.f.). ¿Qué es el marco MITRE ATT&CK? Recuperado el 22 de marzo de 2024, de https://www.ibm.com/mx-es/topics/mitre-attack

MITRE Corporation. (s.f.). Resources. Recuperado el 22 de marzo de 2024, de https://attack.mitre.org/resources