Anàlisi d'Amenaces Usant la Matriu MITRE ATT&CK (Enterprise, Mobile i ICS)

Objectiu de la pràctica

1. Aprendre a utilitzar la matriu MITRE ATT&CK per identificar tàctiques i tècniques associades a diferents entorns: **Enterprise, Mobile i ICS** (**Industrial Control Systems)**.

2. Relacionar tàctiques i tècniques amb mesures de prevenció i detecció.

3. Desenvolupar habilitats per navegar per la matriu ATT&CK i identificar informació clau.

Escenari i requisits

L'organització fictícia **TechSecure** opera en tres àrees:

- **Enterprise**: Xarxes corporatives amb estacions de treball Windows i servidors basats en el núvol.

- **Mobile**: Dispositius mòbils Android utilitzats pels empleats per accedir a aplicacions empresarials.

- **ICS**: Sistemes de control industrial que supervisen i gestionen línies de producció.

TechSecure vol millorar la seva seguretat investigant com un atacant podria comprometre cadascun d'aquests entorns i quines mesures podrien implementar per protegir-se.

Part 1: Anàlisi per a l'entorn Enterprise

- S'han detectat intents d'accés no autoritzat a una plataforma de núvol utilitzada per l'organització.

- Es sospita que els atacants intenten robar credencials per accedir al sistema.

Activitats:

- Accedir a la matriu ATT&CK Enterprise https://attack.mitre.org/matrices/enterprise/

- Buscar una tècnica sota la tàctica 'Credential Access' que pugui ser utilitzada per robar credencials (ex.: Credential Dumping).

- Investigar com funciona aquesta tècnica i proposar:

  - Mesures preventives (Mitigations).

  - Mesures de detecció.

Part 2: Anàlisi per a l'entorn Mobile

- Un empleat ha instal·lat una aplicació no autoritzada en el seu dispositiu Android. Es sospita que l'aplicació podria comprometre dades empresarials sensibles.

Activitats:

- Accedir a la matriu ATT&CK Mobile https://attack.mitre.org/matrices/mobile/

- Buscar una tècnica sota la tàctica 'Initial Access' que expliqui com una aplicació maliciosa podria aconseguir accés al dispositiu.

- Proposar:

  - Mesures preventives (Mitigations).

  - Mesures de detecció.

Part 3: Anàlisi per a l'entorn ICS

- Un atacant ha accedit a la xarxa de l'empresa i està intentant enviar comandes malicioses a un PLC (Programmable Logic Controller) per alterar el procés industrial.

Activitats:

- Accedir a la matriu ATT&CK ICS https://attack.mitre.org/matrices/ics/

- Buscar una tècnica sota la tàctica 'Execution' que pugui ser utilitzada per manipular PLCs.

- Proposar:

  - Mesures preventives (Mitigations).

  - Mesures de detecció.