01. Trabajo en grup

Created by: @raf181_ | Date: `07-12-2024`

1. Representación de la red como un grafo

Estructura del grafo:

- **Nodos (V):** Representan los dispositivos de la red.
  - $S_1, S_2, \ldots, S_m$: Nodos de distribución (switches).
  - $P_1, P_2, \ldots, P_n$: Endpoints (PCs).
- **Aristas (E):** Representan las conexiones entre dispositivos.
  - Si un switch S_i está conectado a un endpoint P_j, existe una arista $(S_i, P_j) \in E$.
  - Las aristas pueden tener pesos w_{ij}, que representan factores como ancho de banda o probabilidad de propagación de malware.

El grafo puede ser dirigido o no dirigido:

- **No dirigido** si las conexiones son simétricas (ej., cable Ethernet).
- **Dirigido** si el malware tiene direccionalidad (ej., ataques específicos).

2. Modelo matemático de propagación

Modelo SIR adaptado:

Cada nodo tiene uno de los siguientes estados:

- **Susceptible (S):** El nodo puede ser infectado.
- **Infectado (I):** El nodo está infectado y puede propagar el malware.
- **Recuperado (R):** El nodo ya no puede ser infectado (se ha desinfectado o está aislado).

Diferenciales del modelo SIR:

- $S(t)$: Fracción de nodos susceptibles en el tiempo t.
- $I(t)$: Fracción de nodos infectados en el tiempo t.
- $R(t)$: Fracción de nodos recuperados en el tiempo t.

El modelo se describe con estas ecuaciones diferenciales:

$$\frac{dS}{dt} = -\beta SI$$

$$\frac{dI}{dt} = \beta SI - \gamma I$$

$$\frac{dR}{dt} = \gamma I$$

Donde:

- β: Tasa de propagación del malware (depende de $wijw_{ij}$).
- γ: Tasa de recuperación (ej., desinfección).

3. Cálculo de métricas clave en el grafo

Centralidad de grado:

Identifica nodos que tienen muchas conexiones:

Grado de un nodo $v_i = \deg(v_i) = \sum_j A_{ij}$

donde A_{ij} es el elemento de la matriz de adyacencia (1 si hay una conexión entre i y j, 0 en caso contrario).

- Los switches suelen tener grados altos, lo que los hace vulnerables para propagar el malware rápidamente.

Centralidad de intermediación:

Identifica nodos clave en las rutas:

$$CB(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

donde:

- σ_{st}: Número total de caminos más cortos entre s y t.
- $\sigma_{st}(v)$: Número de esos caminos que pasan por v.

Un switch con alta centralidad de intermediación puede ser un punto crítico en la propagación.

Centralidad de cercanía:

Mide qué tan cerca está un nodo de todos los demás:

$$C_C(v) = \frac{1}{\sum_{u \in V} d(v,u)}$$

donde $d(v,u)$ es la distancia geodésica (número de aristas en el camino más corto entre v y u).

- Los switches con baja distancia geodésica hacia otros nodos son importantes para contener el malware.

---

4. Simulación de propagación

Paso 1: Inicialización

- Seleccionar un nodo inicial infectado (ej., un endpoint comprometido por un phishing).
- Asignar probabilidades de propagación β_{ij} entre nodos.

Paso 2: Iteraciones

1. Para cada nodo infectado v:
   - Infectar a sus nodos vecinos con probabilidad β_{ij}.
   - Mover v al estado "Recuperado" con probabilidad γ\gamma.
2. Actualizar los estados $S(t), I(t), R(t)$ en cada iteración.
3. Continuar hasta que $I(t) \approx 0$ (el malware deja de propagarse).

Visualización:

- Graficar $S(t), I(t), R(t)$ en función del tiempo.
- Mostrar la red con los estados de los nodos usando colores (verde: susceptible, rojo: infectado, azul: recuperado).

---

5. Estrategias de contención

Puedes analizar cómo afectan las siguientes estrategias:

1. **Aislar nodos clave:** Desconectar switches con alta centralidad de intermediación.
2. **Priorizar parches:** Actualizar nodos con alta centralidad de grado.
3. **Segmentación de la red:** Dividir la red en subgrafos para contener el malware.
