BARBHACK 2020

PROPAGATION DE L'IMPACT DES VULNÉRABILITÉS DANS LES SYSTÈMES COMPLEXES

Antoine Boudermine

29/08/2020

QUI SUIS-JE?

Prénom : Antoine
Nom : Boudermine
Age : 24 ans

antoine.boudermine@protonmail.com
https://www.linkedin.com/in/antoine-boudermine-678ab0152

Effectue une thèse au CERT Naval Group sur le sujet suivant:

« Etude de la propagation de l'impact des vulnérabilités dans les systèmes complexes »

INTRODUCTION

INTRODUCTION
MISSION

Concevoir

Réaliser

Entretenir

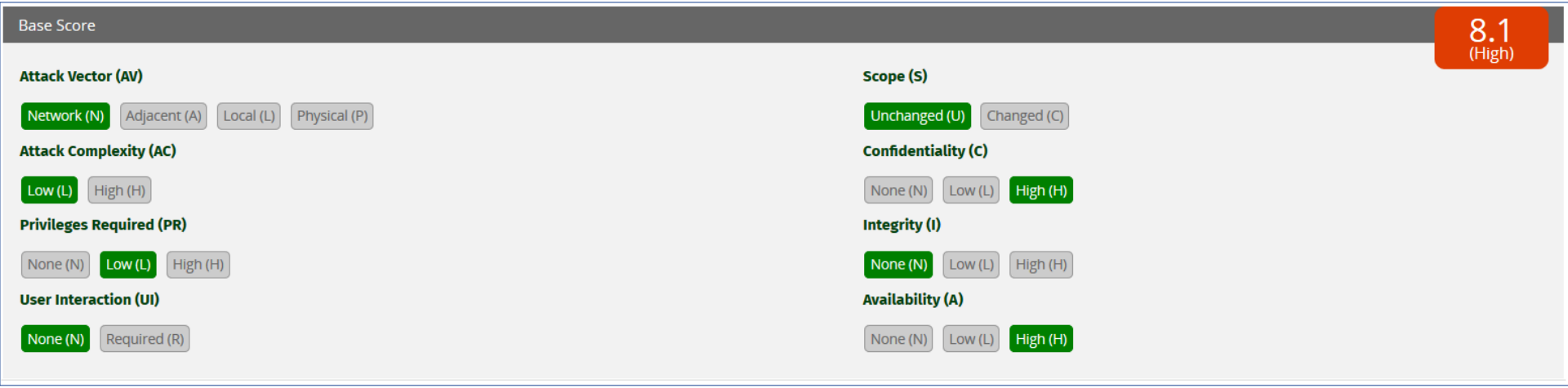
INTRODUCTION
PROBLÉMATIQUE

Compatibilités des produits

Mise à jour sans connexion

Perturbation de la mission

INTRODUCTION
CVSS SCORE



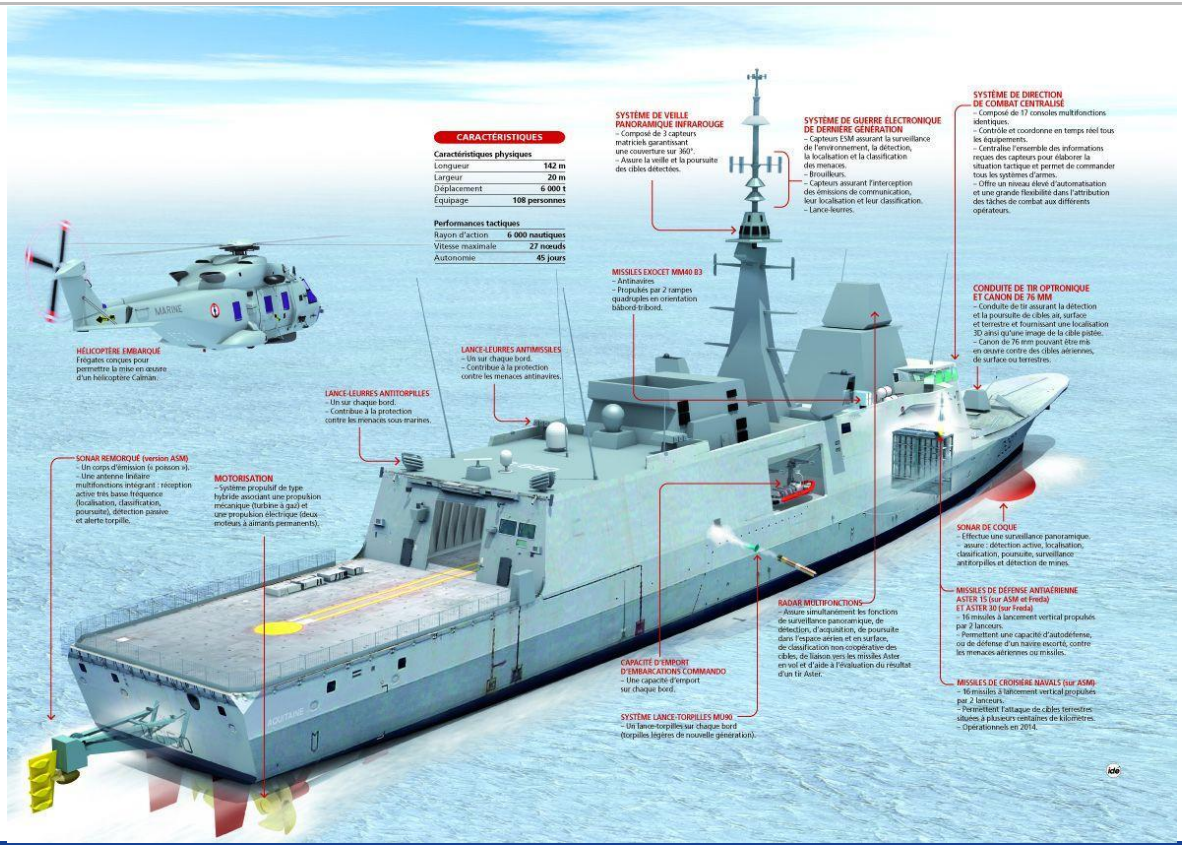
Impact sur le système ?

INTRODUCTION
SYSTÈME COMPLEXE

Nombreux éléments hétérogènes

Fortes interactions

Evolution au cours du temps

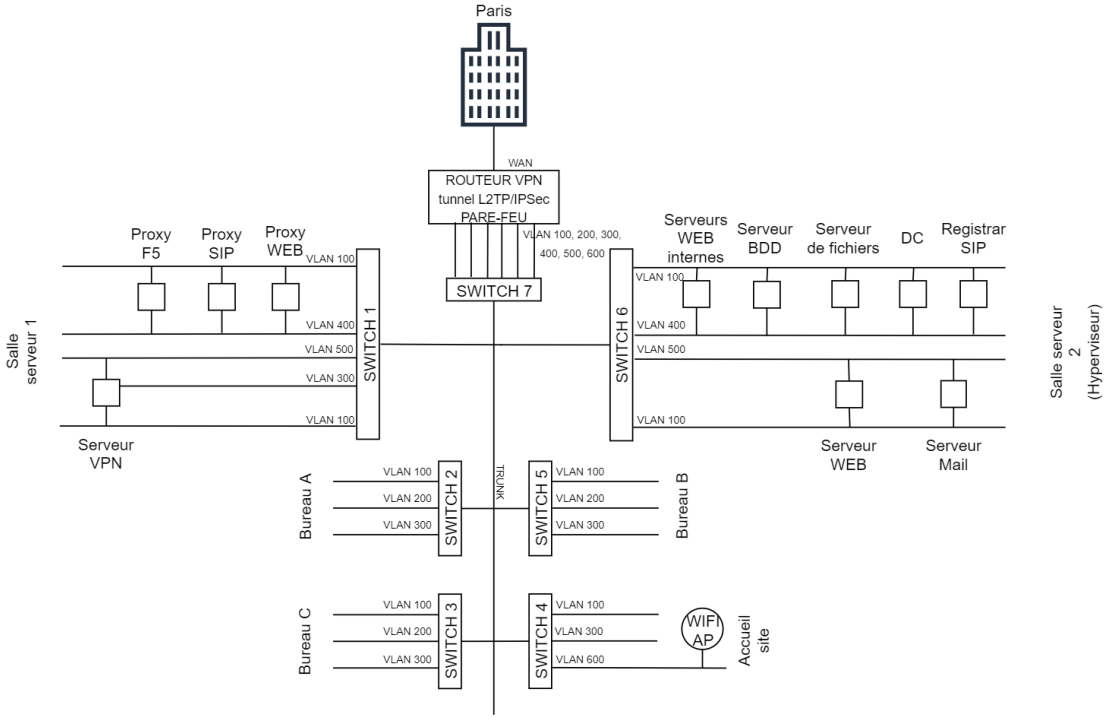


Comment résoudre ce problème ?

Identifier l'importance de l'élément dans la structure du système.

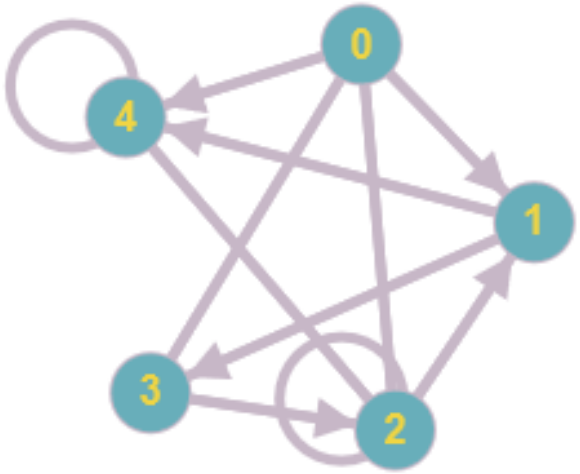
Identifier les différents scénarios d'attaques permettant d'exploiter la vulnérabilité.

INTRODUCTION
EXEMPLE D'UN SYSTÈME COMPLEXE



SOLUTIONS EXISTANTES

SOLUTIONS EXISTANTES
PRÉREQUIS

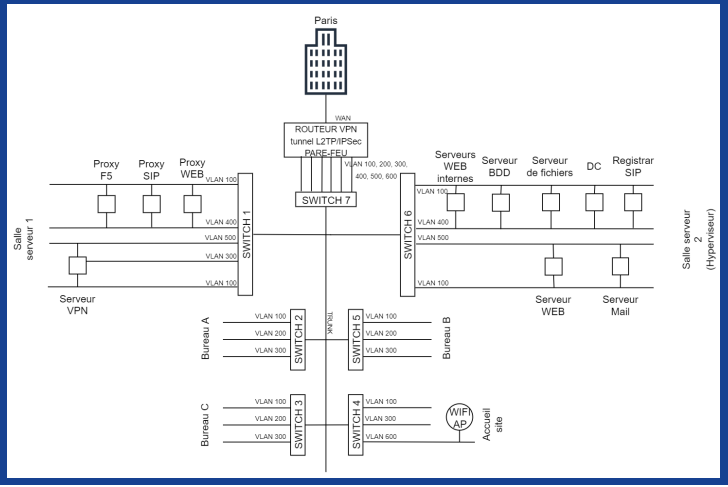


Matrice d'adjacence

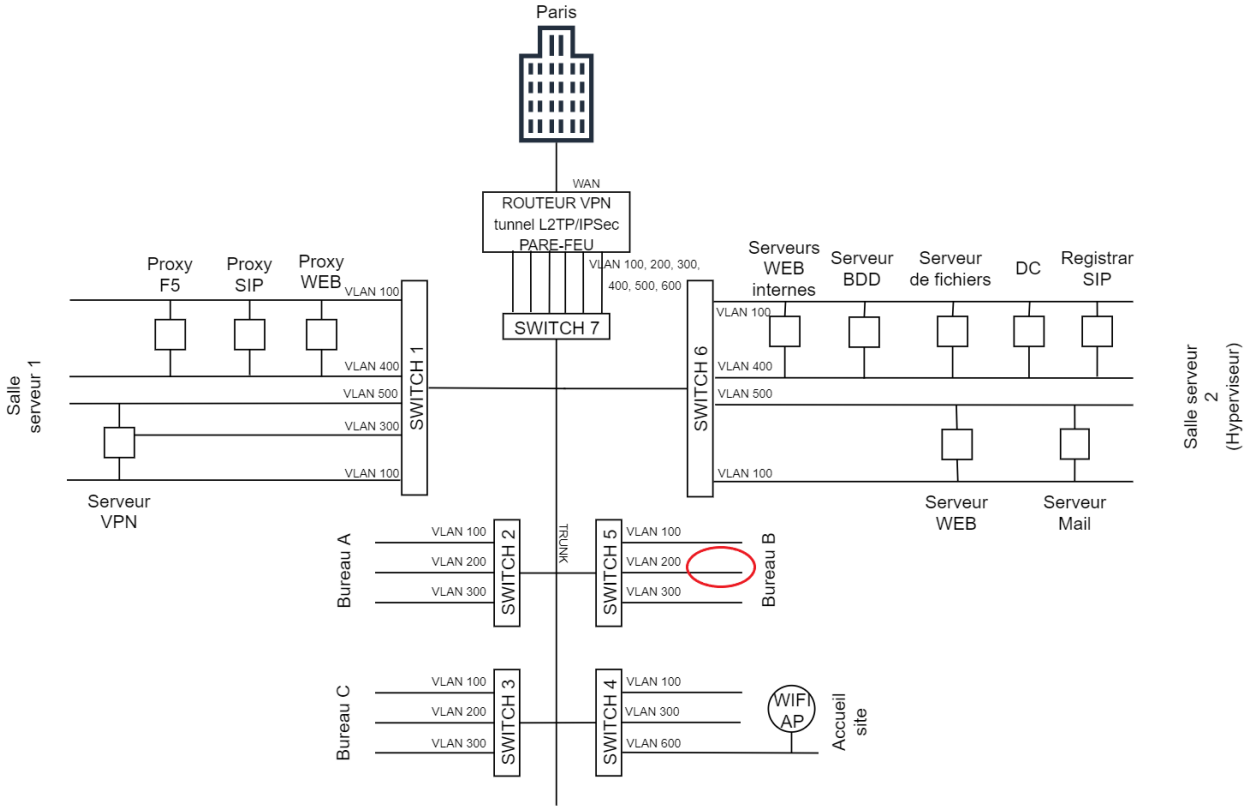
$$A = \begin{array}{c} \\ From \end{array} \begin{array}{c} \begin{array}{ccccc} & & & To & \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

SOLUTIONS EXISTANTES

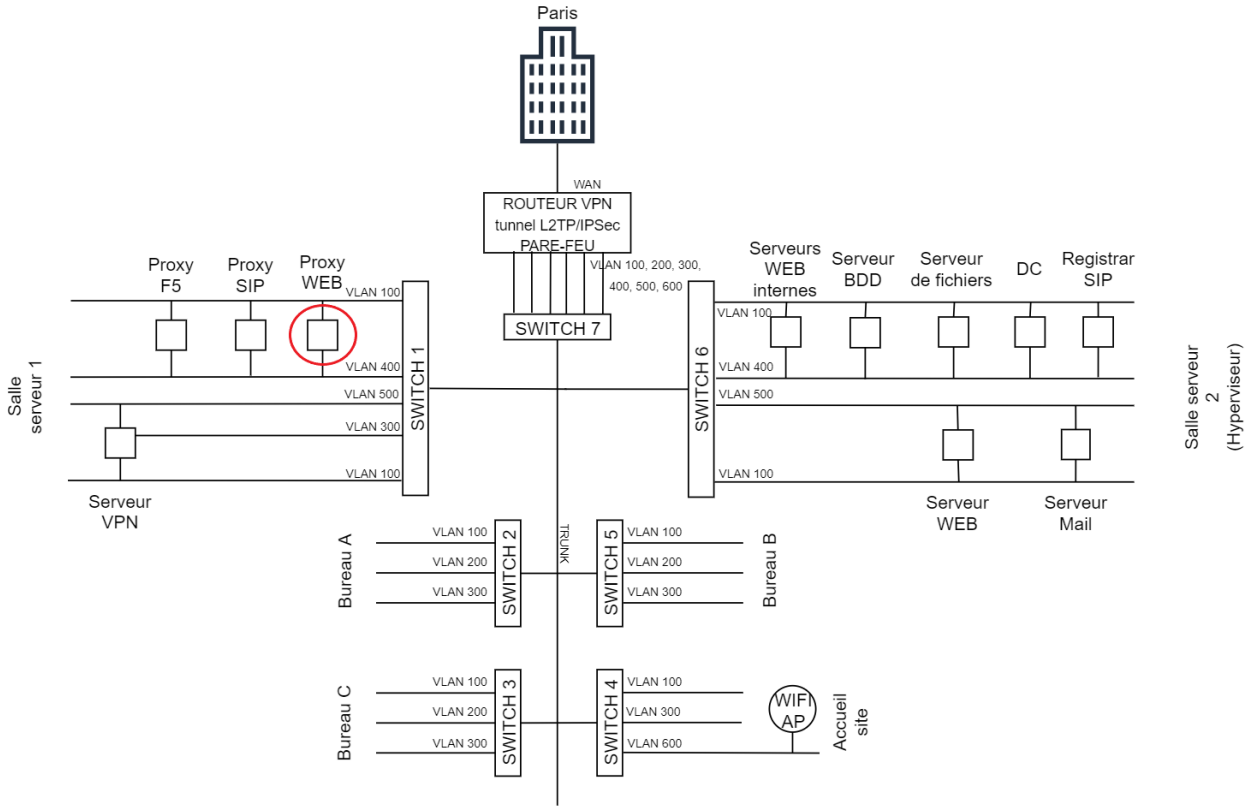
ANALYSE STRUCTURELLE DU SYSTÈME



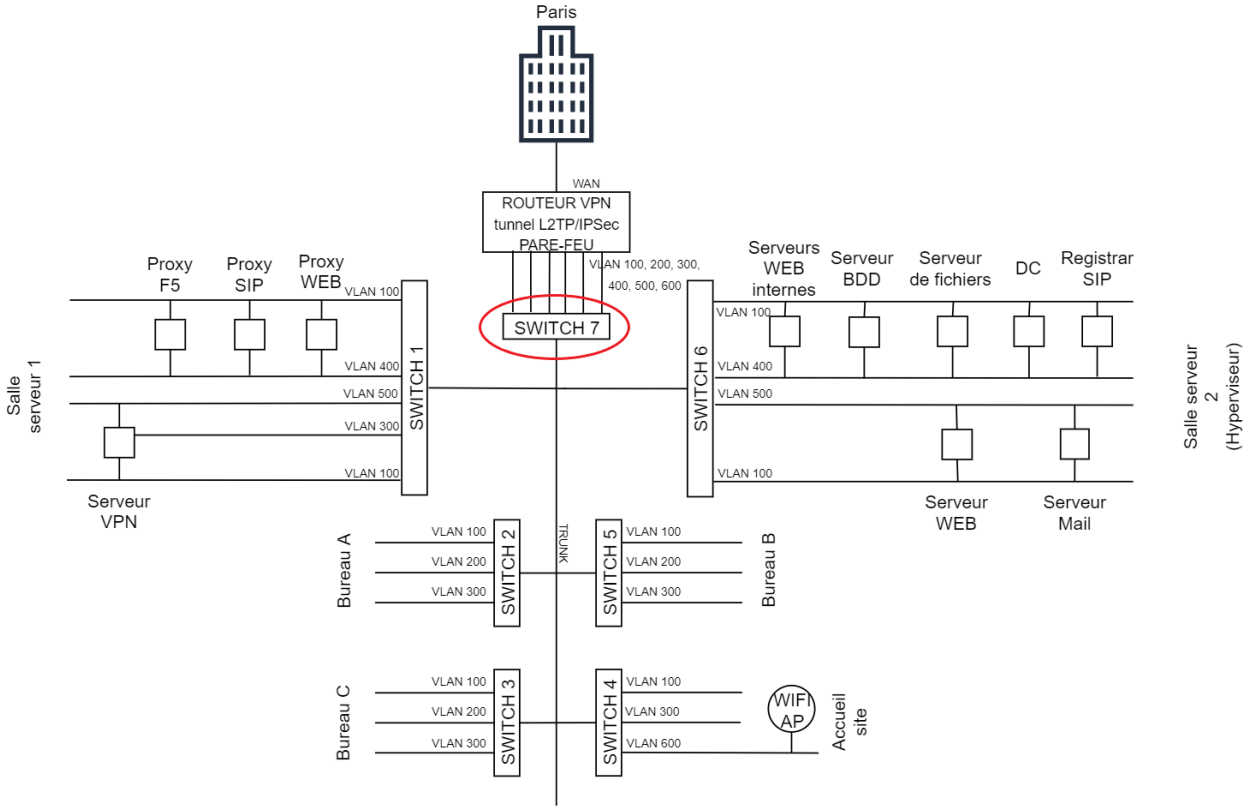
SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME



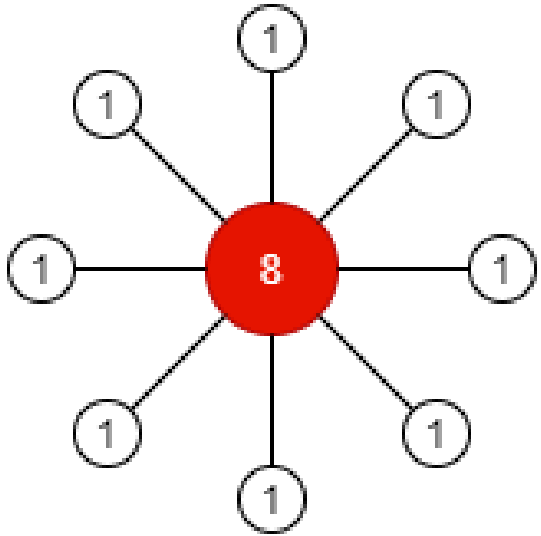
SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Degree centrality

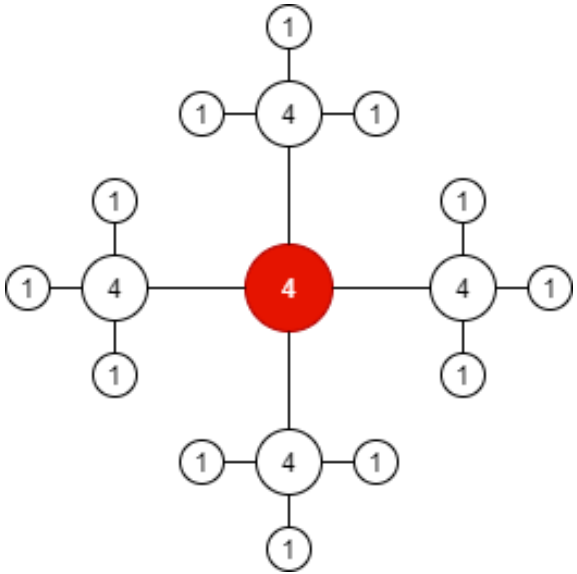
$$ND_i = \sum_{j=1, j \neq i}^{N} a_{ij}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Eigenvector centrality

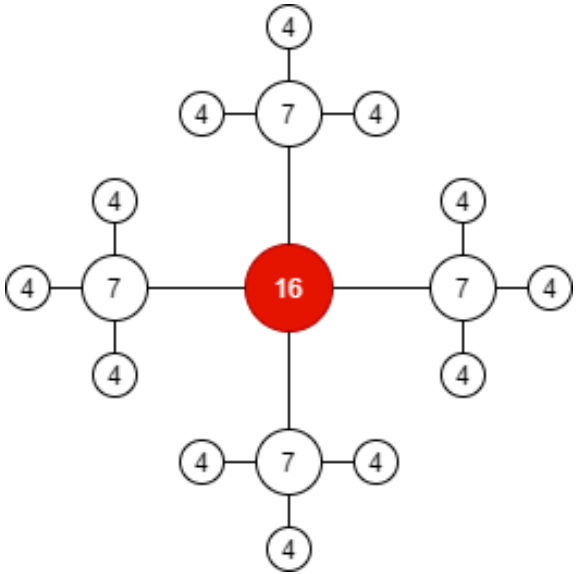
$$A \times \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \\ \vdots \\ 4 \end{bmatrix}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Eigenvector centrality

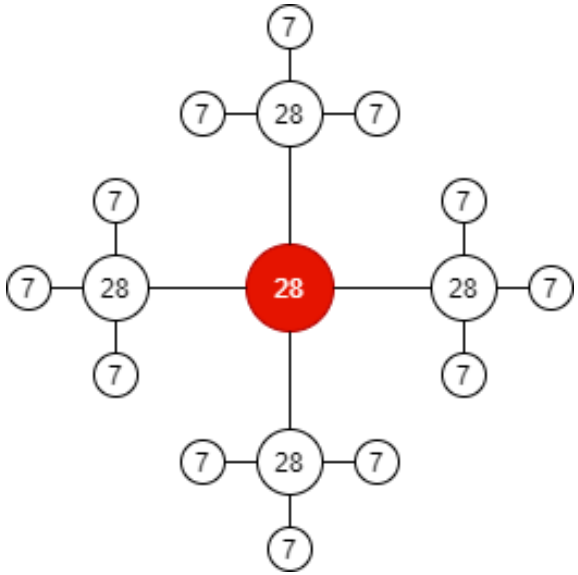
$$A \times \begin{bmatrix} 1 \\ 4 \\ \vdots \\ 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 7 \\ \vdots \\ 16 \end{bmatrix}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Eigenvector centrality

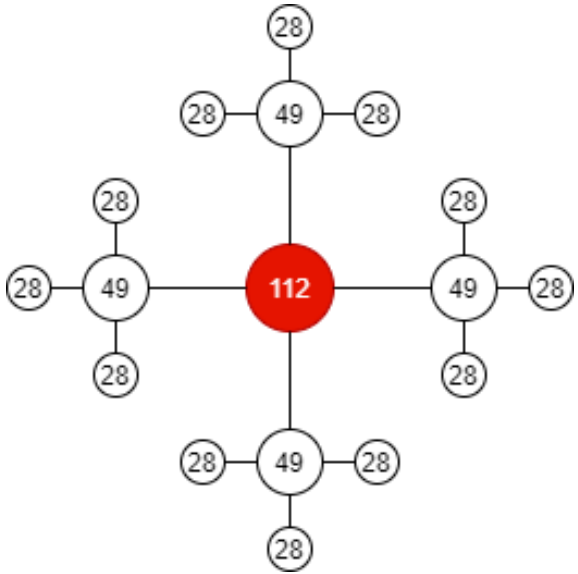
$$A \times \begin{bmatrix} 4 \\ 7 \\ \vdots \\ 16 \end{bmatrix} = \begin{bmatrix} 7 \\ 28 \\ \vdots \\ 28 \end{bmatrix}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Eigenvector centrality

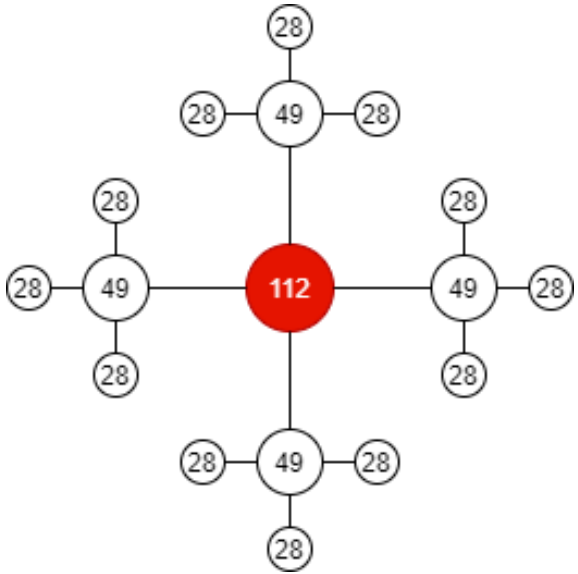
$$A \times \begin{bmatrix} 7 \\ 28 \\ \vdots \\ 28 \end{bmatrix} = \begin{bmatrix} 28 \\ 49 \\ \vdots \\ 112 \end{bmatrix}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Eigenvector centrality

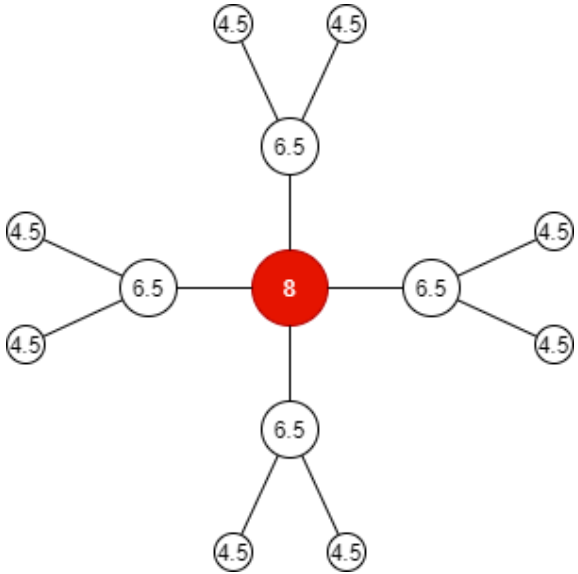
$$A \times \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{bmatrix}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Closeness centrality

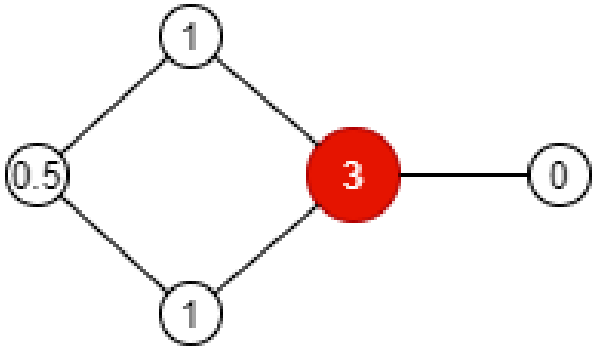
$$C(x) = \sum_{y} \frac{1}{d(x,y)}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

Betweenness centrality

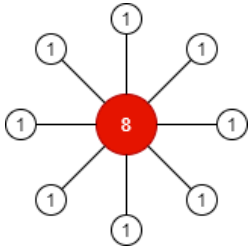
$$\sum_{x \neq y \neq z}^{N} \frac{sp_{yz}(x)}{sp_{yz}}$$



SOLUTIONS EXISTANTES
ANALYSE STRUCTURELLE DU SYSTÈME

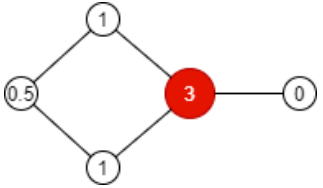
Degree centrality

$$ND_i = \sum_{j=1, j\neq i}^{N} a_{ij}$$



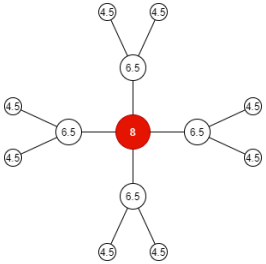
Betweenness centrality

$$BC(x) = \sum_{x\neq y\neq z}^{N} \frac{\omega_{yz}(x)}{\omega_{yz}}$$



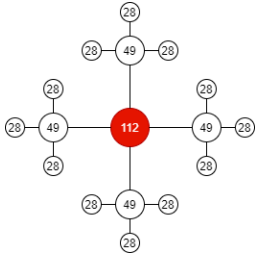
Closeness centrality

$$C(x) = \sum_{y} \frac{1}{d(x,y)}$$



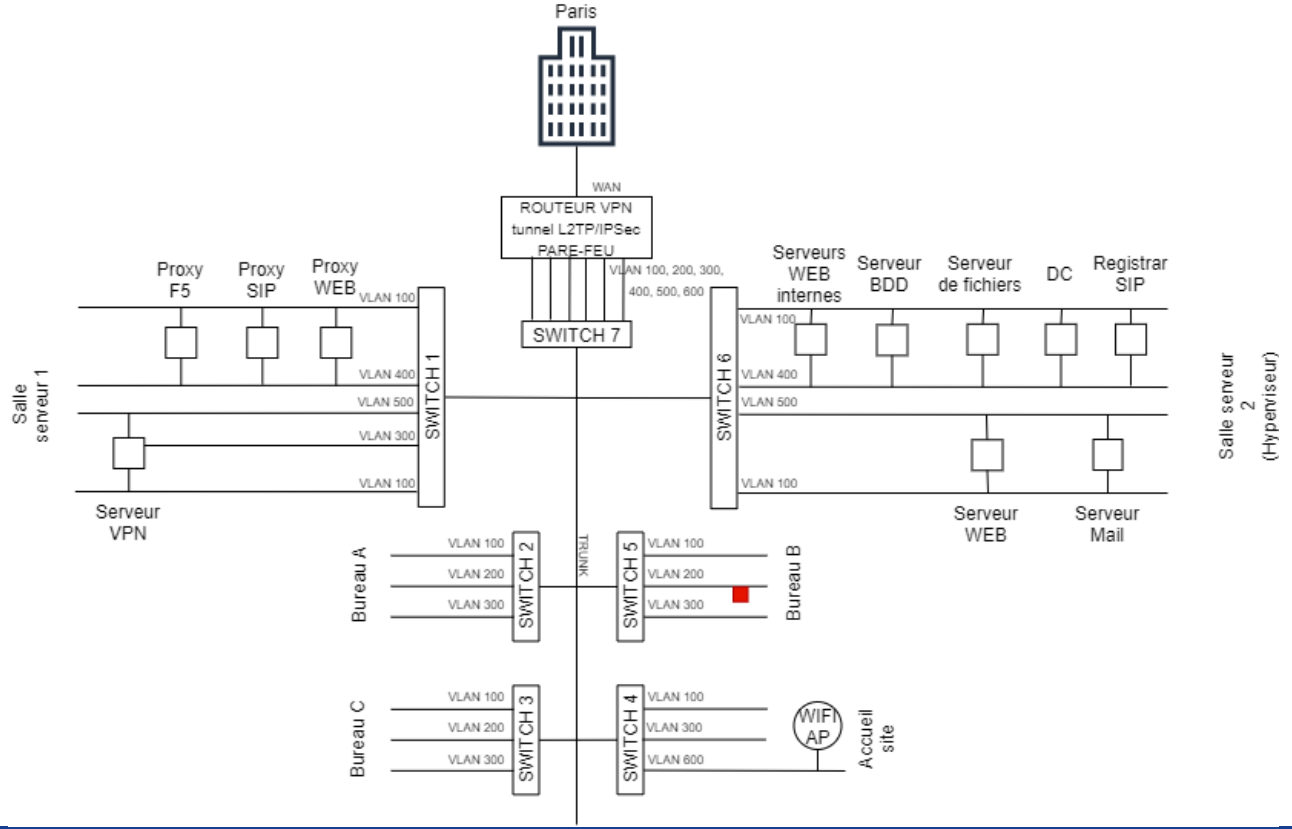
Eigenvector centrality

$$A \times \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{bmatrix}$$



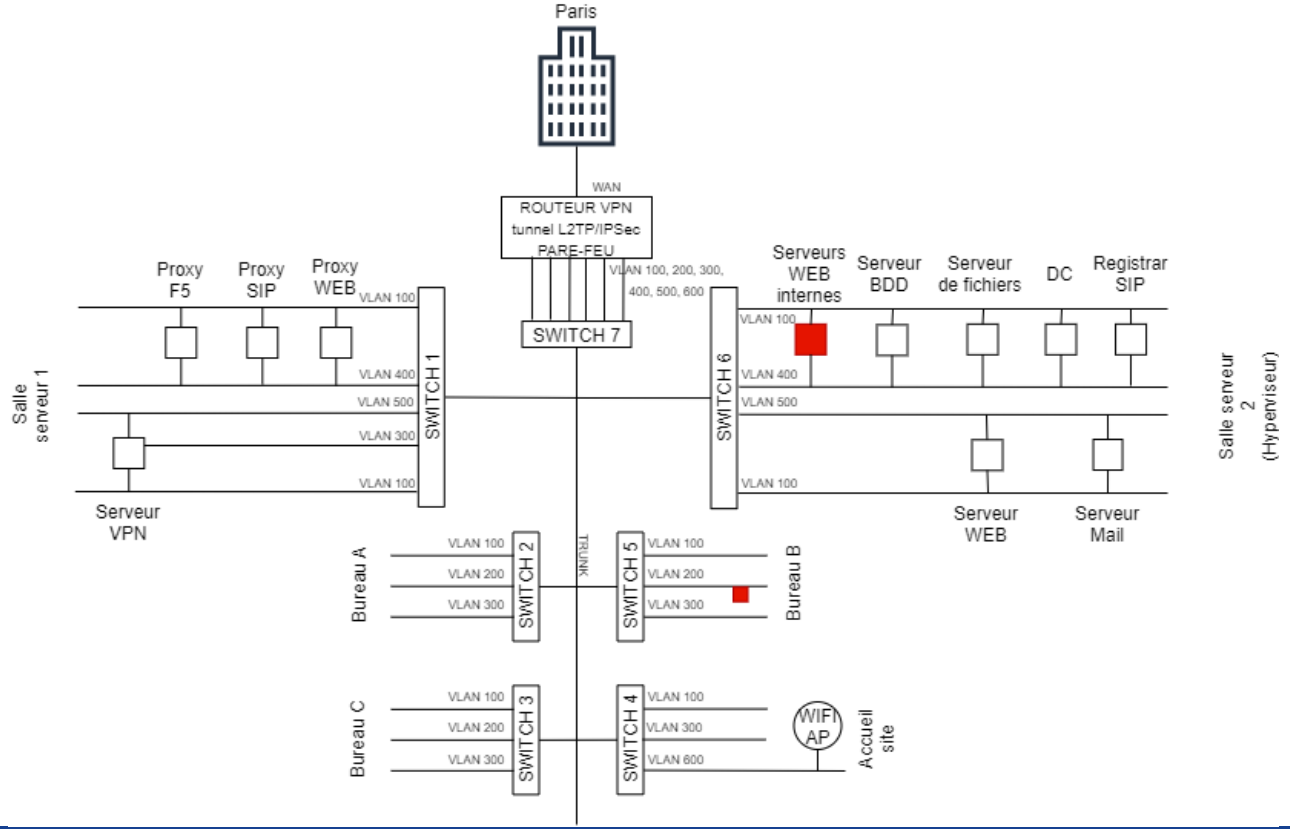
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



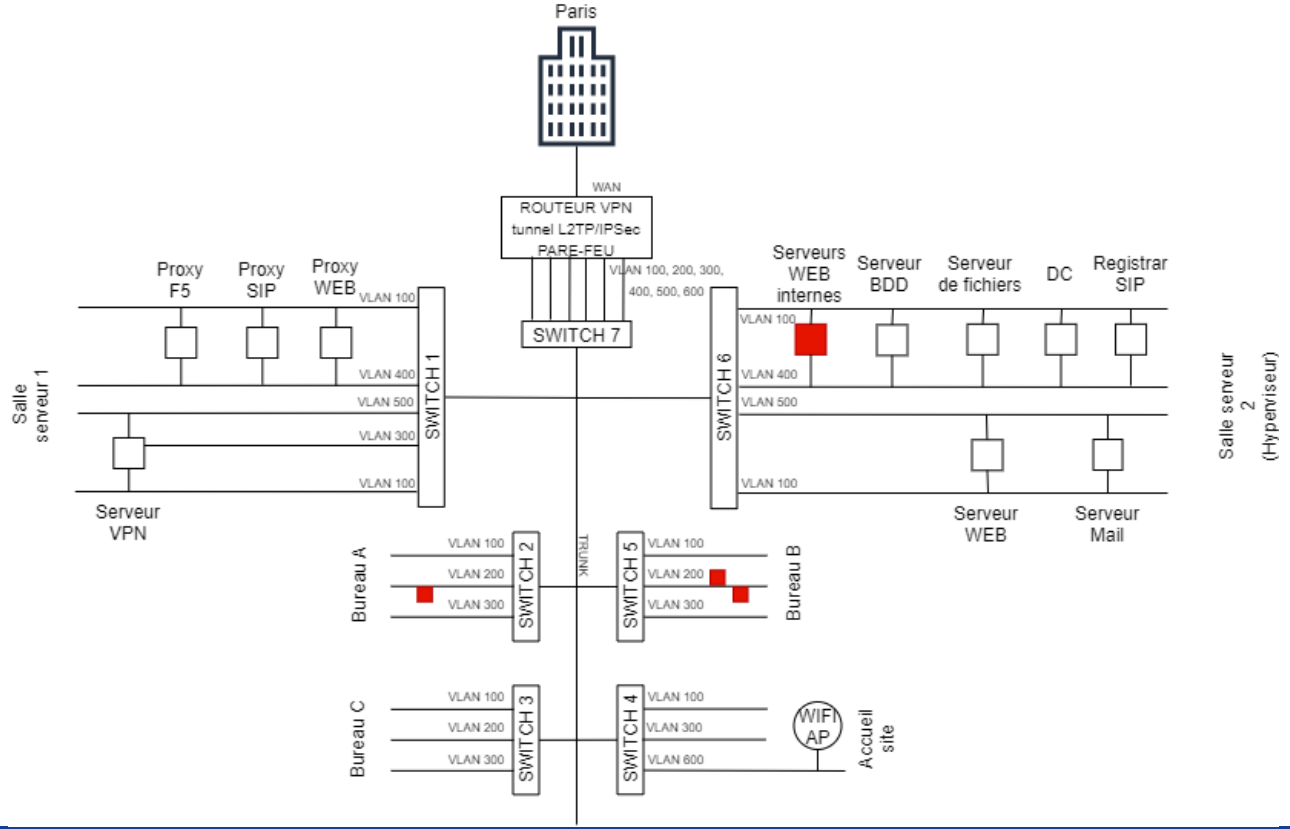
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



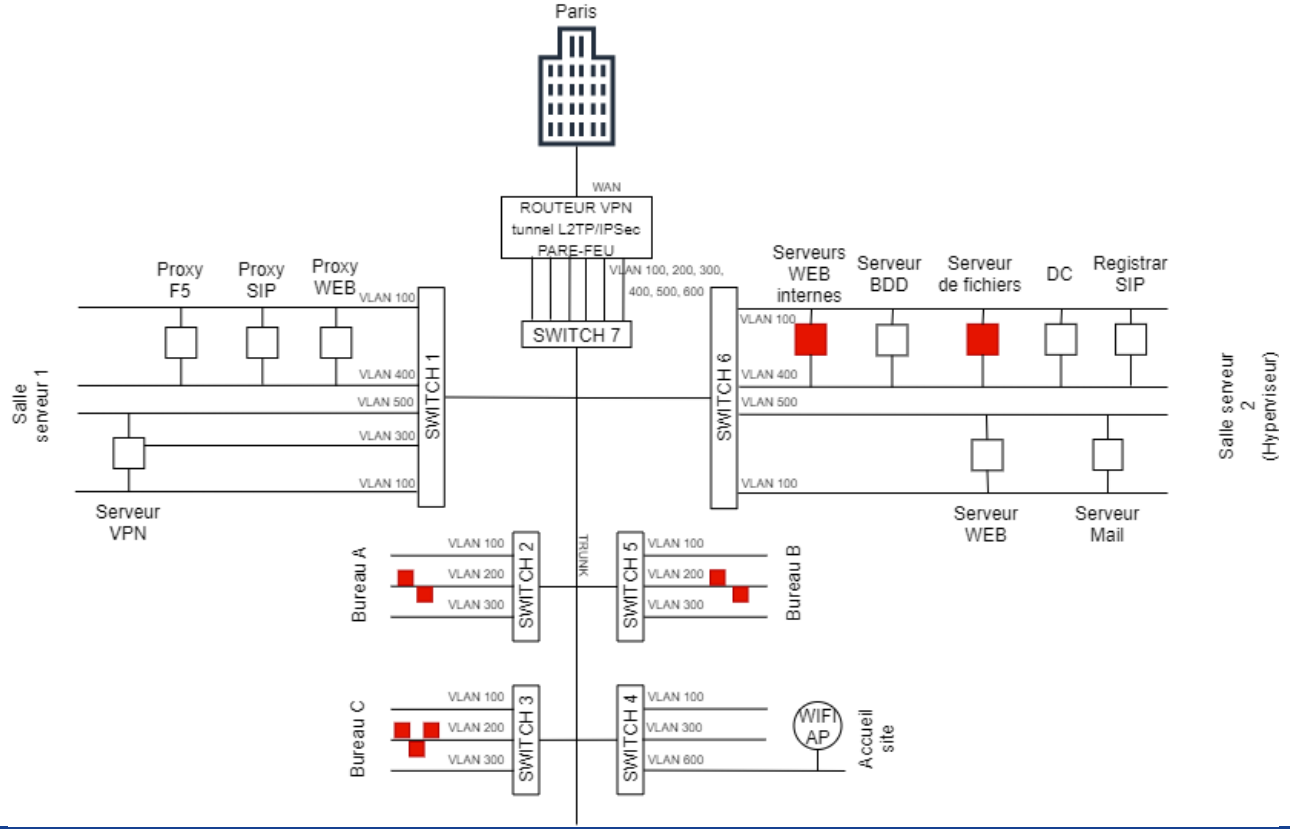
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



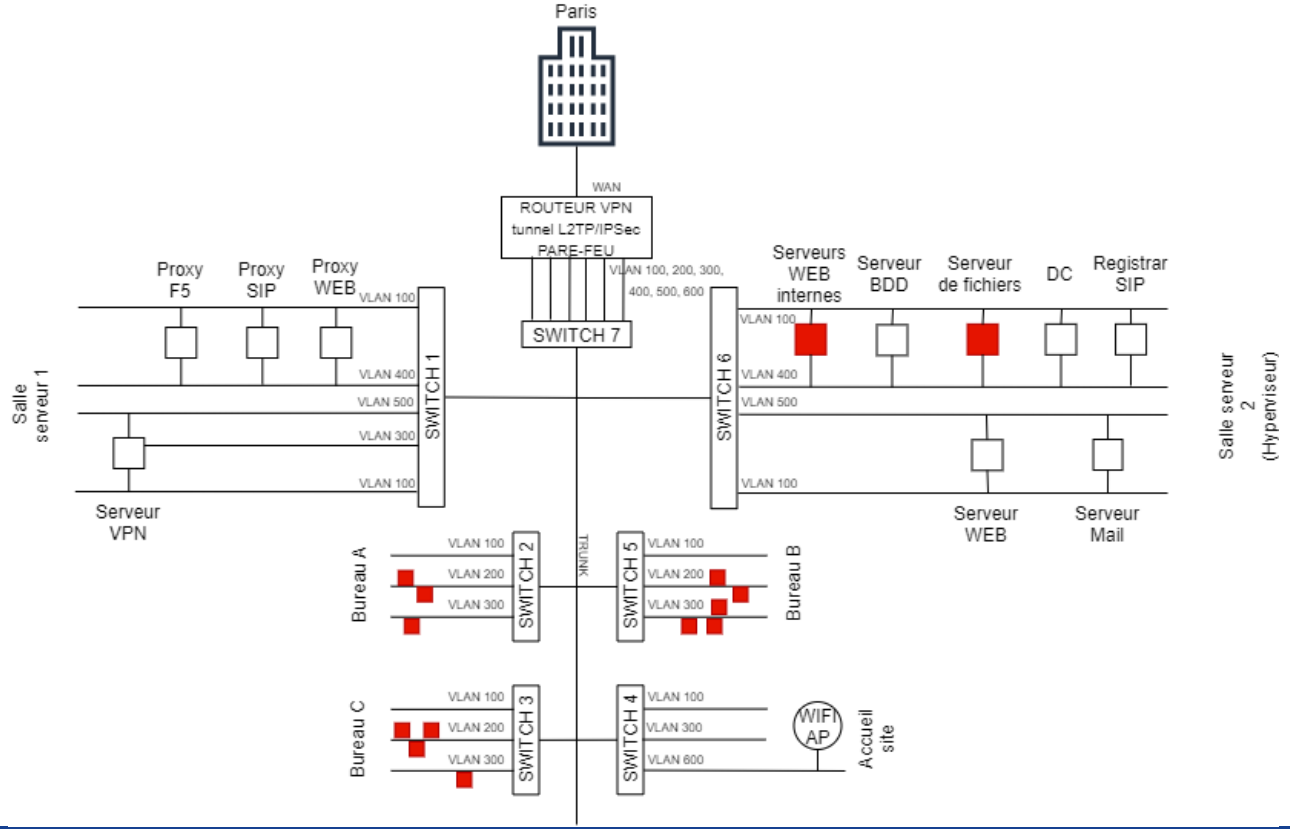
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



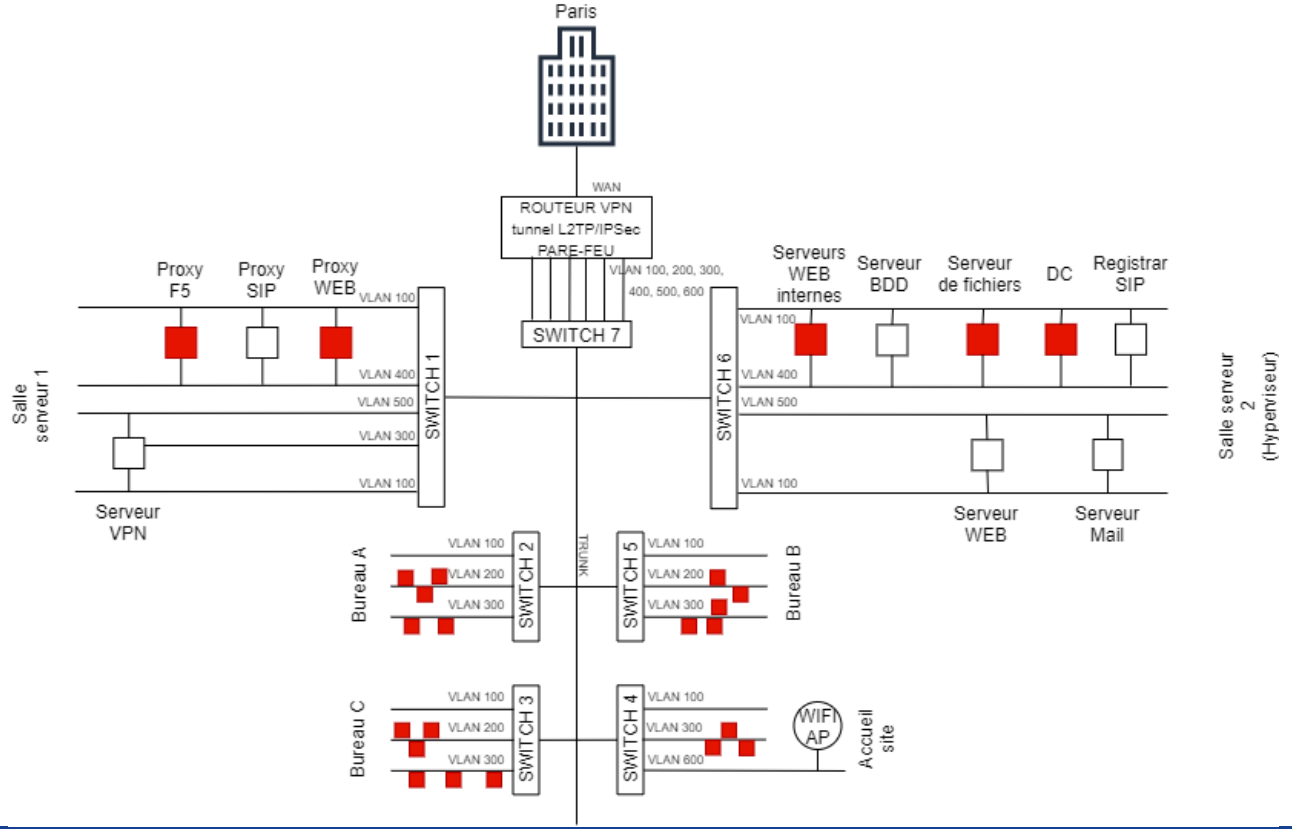
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



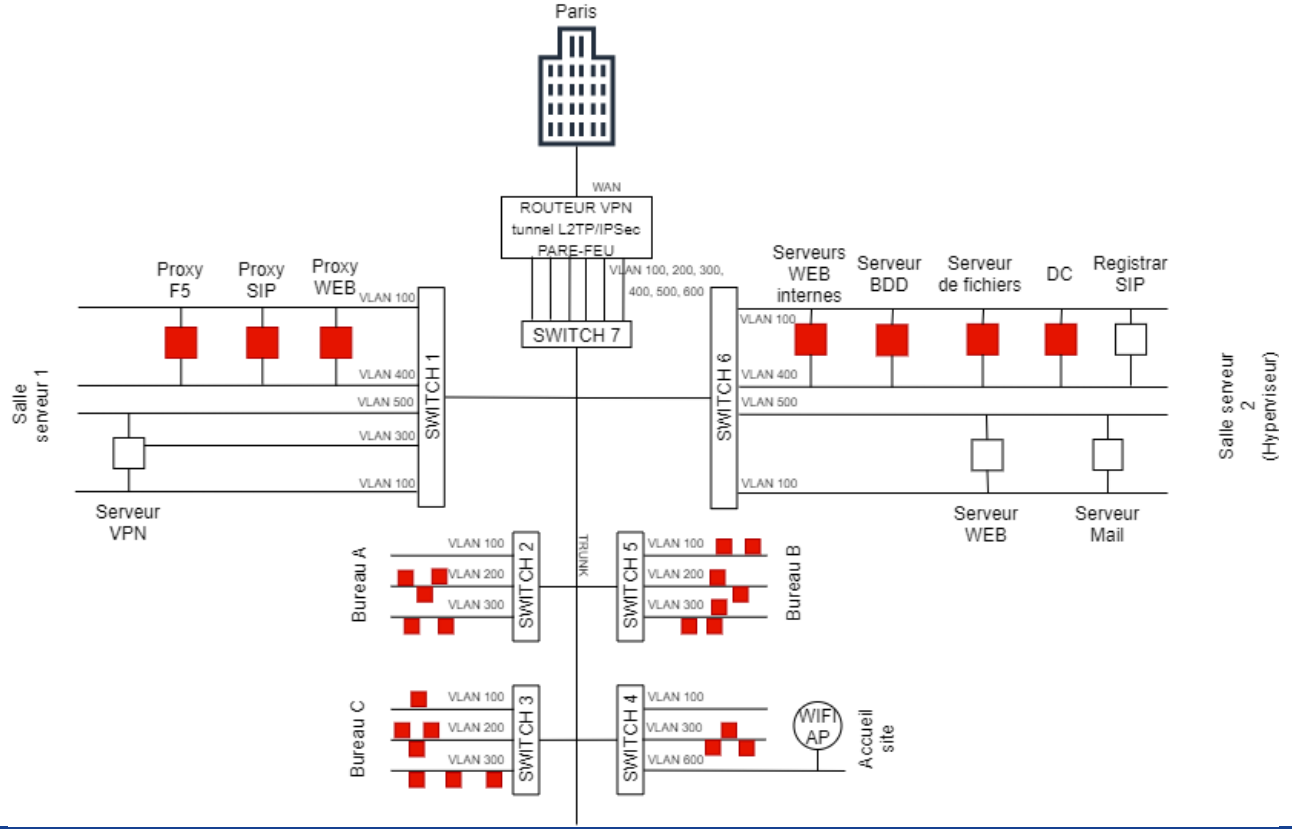
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



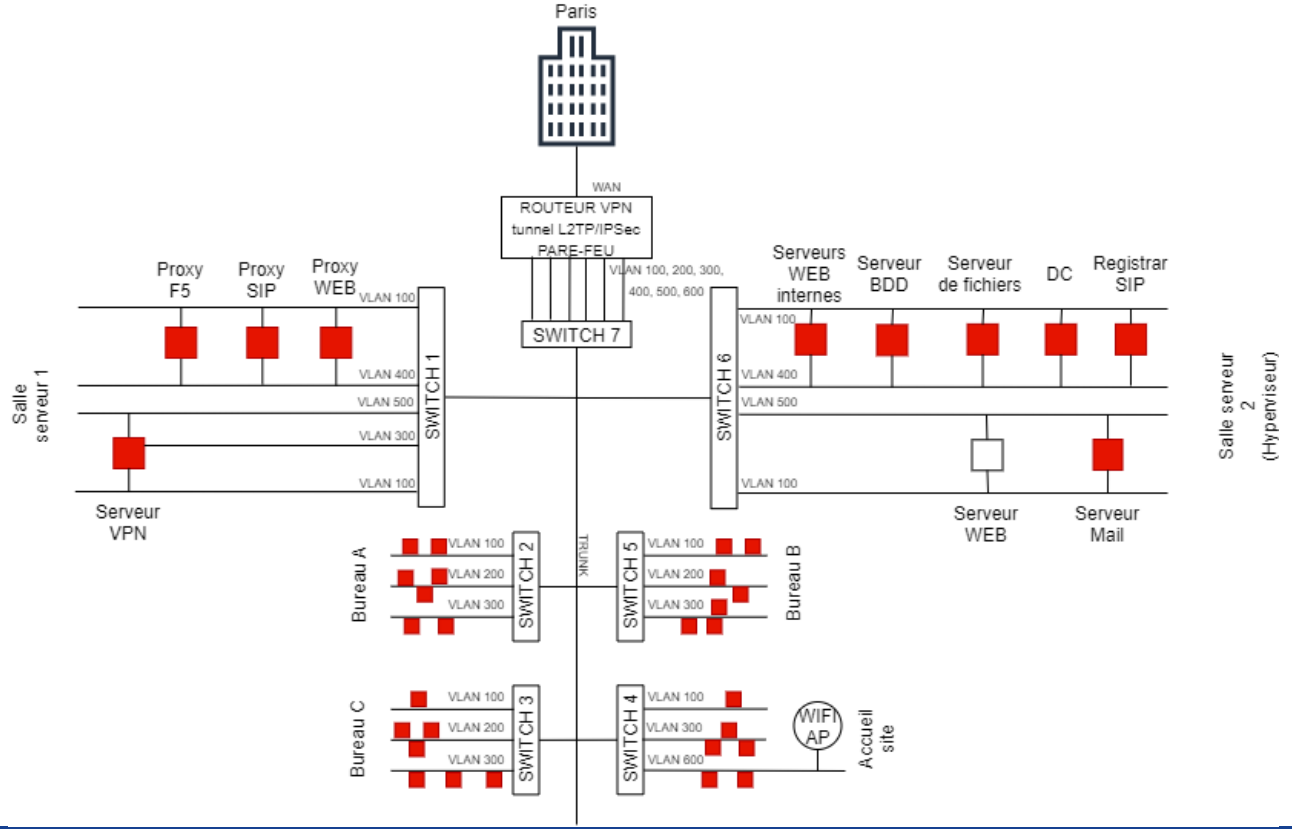
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



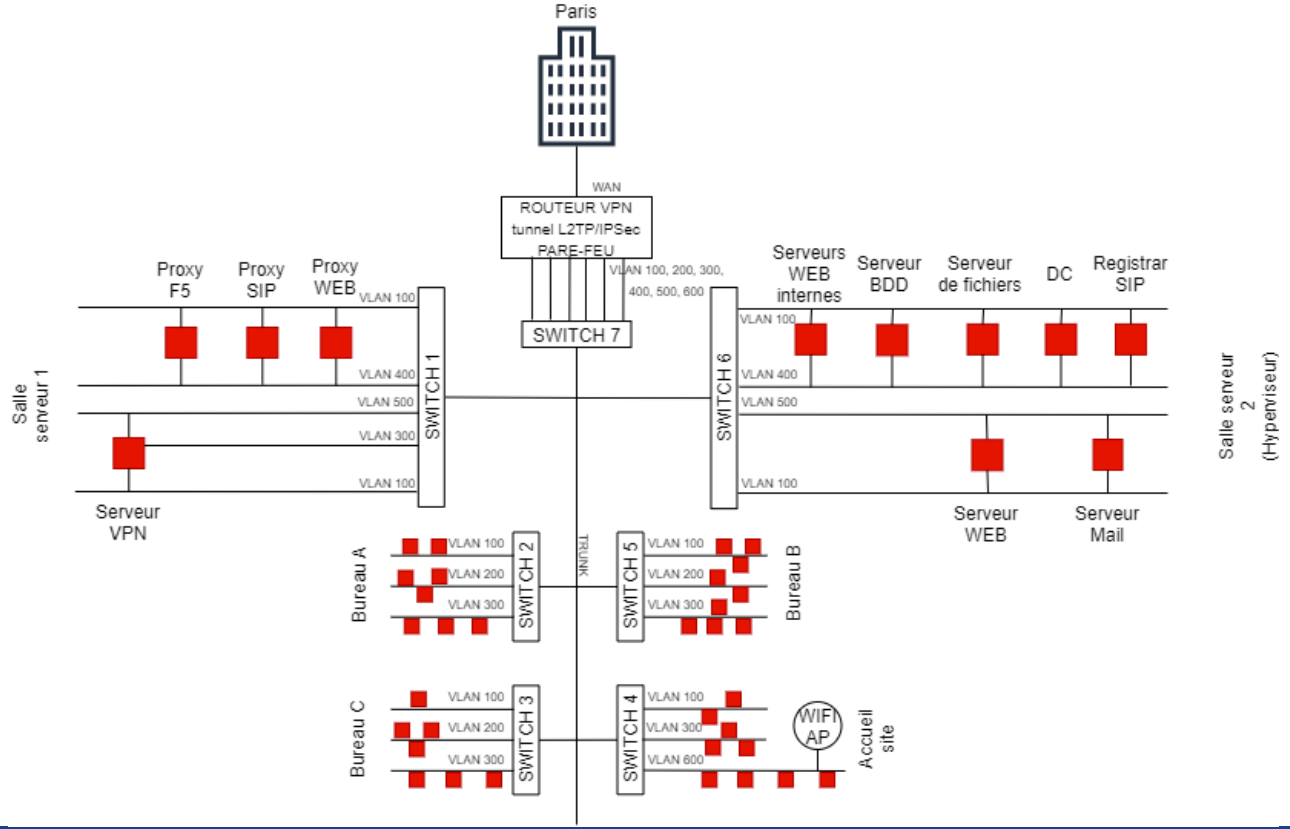
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE



SOLUTIONS EXISTANTES

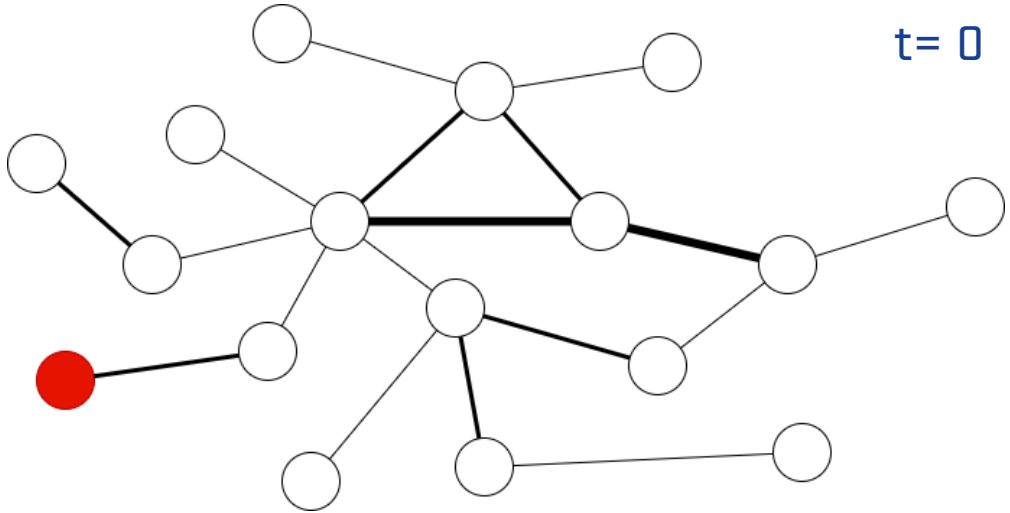
MODÉLISATION DE LA PROPAGATION D'UN MALWARE



SOLUTIONS EXISTANTES

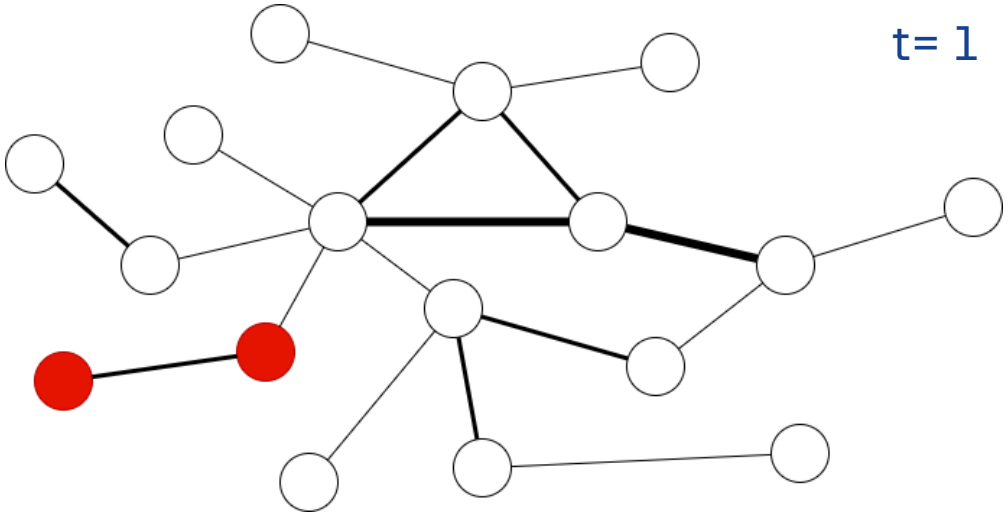
MODÉLISATION DE LA PROPAGATION D'UN MALWARE

1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES
MODÉLISATION DE LA PROPAGATION D'UN MALWARE

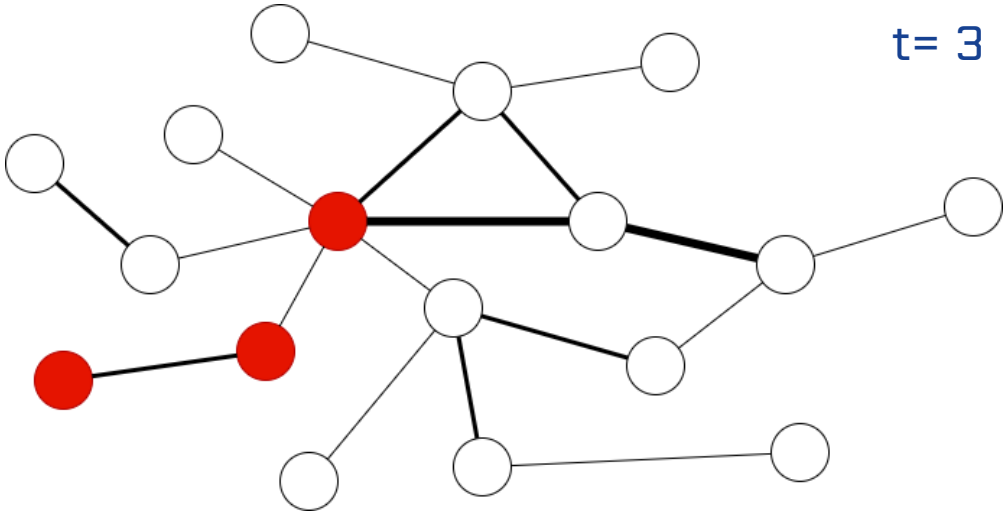
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

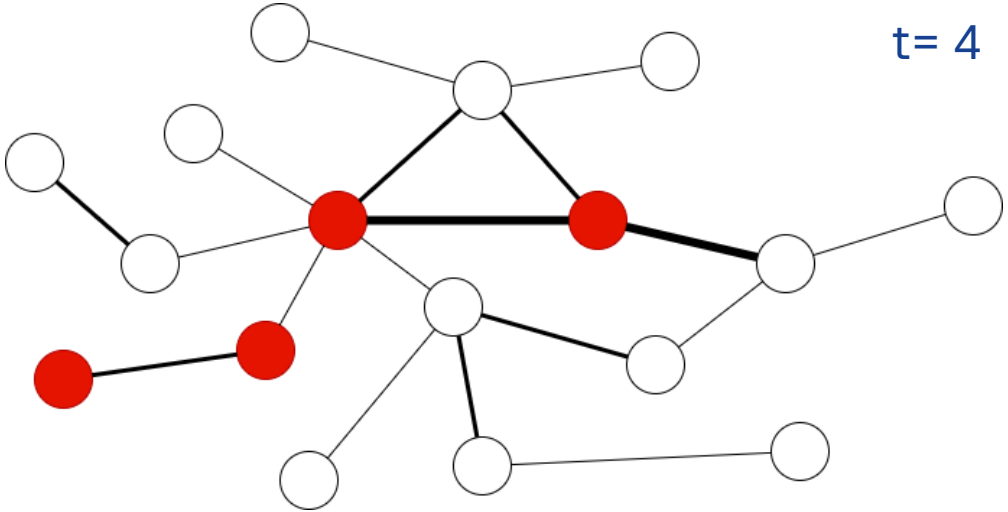
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
   1. La fréquence d'utilisation du lien λ
   2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

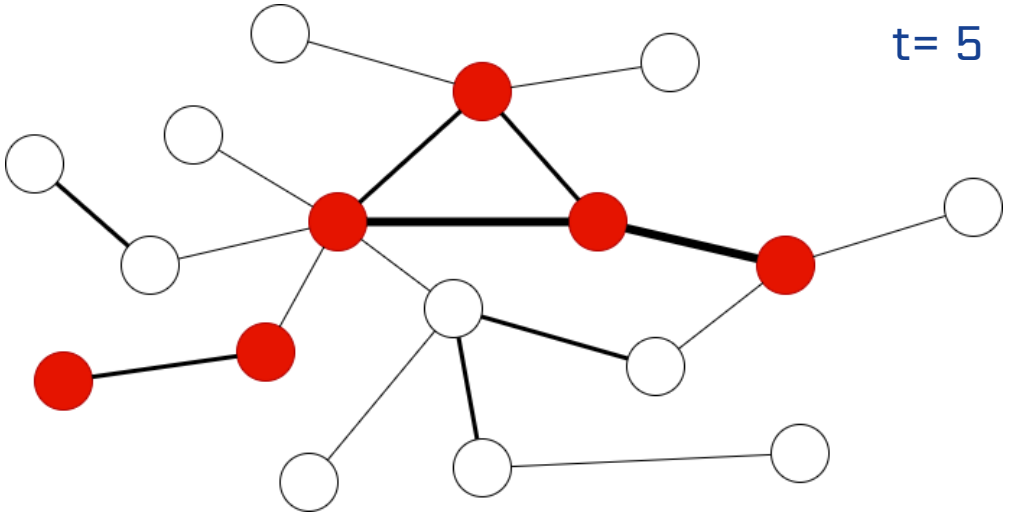
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
   1. La fréquence d'utilisation du lien λ
   2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

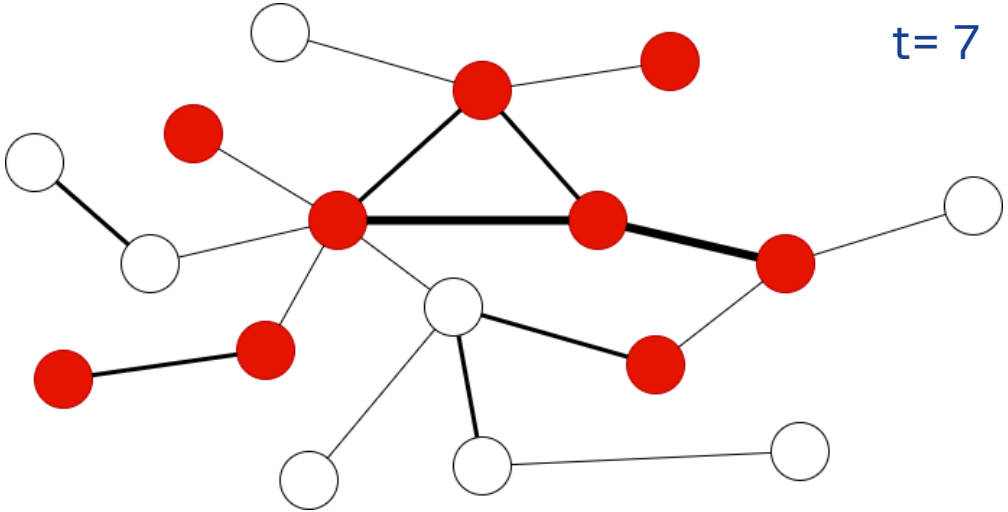
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

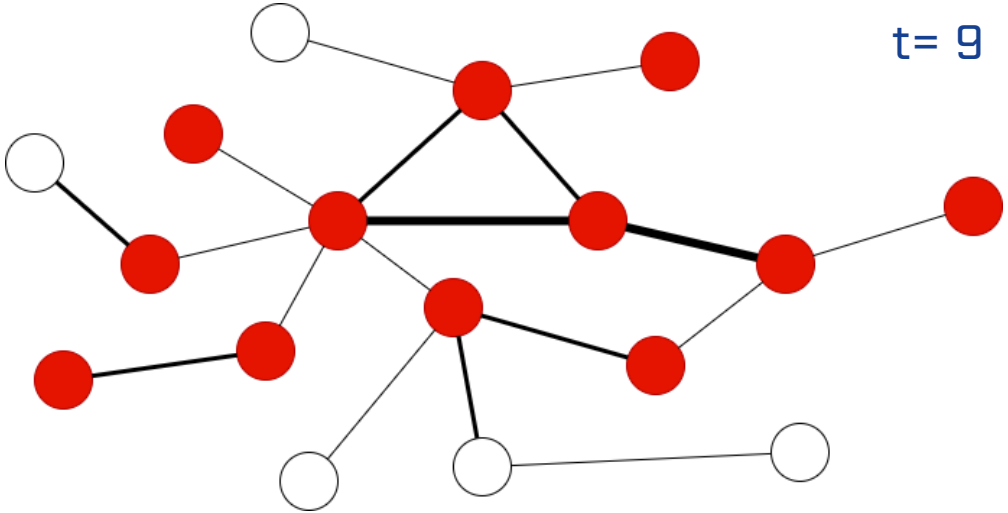
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
   1. La fréquence d'utilisation du lien λ
   2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

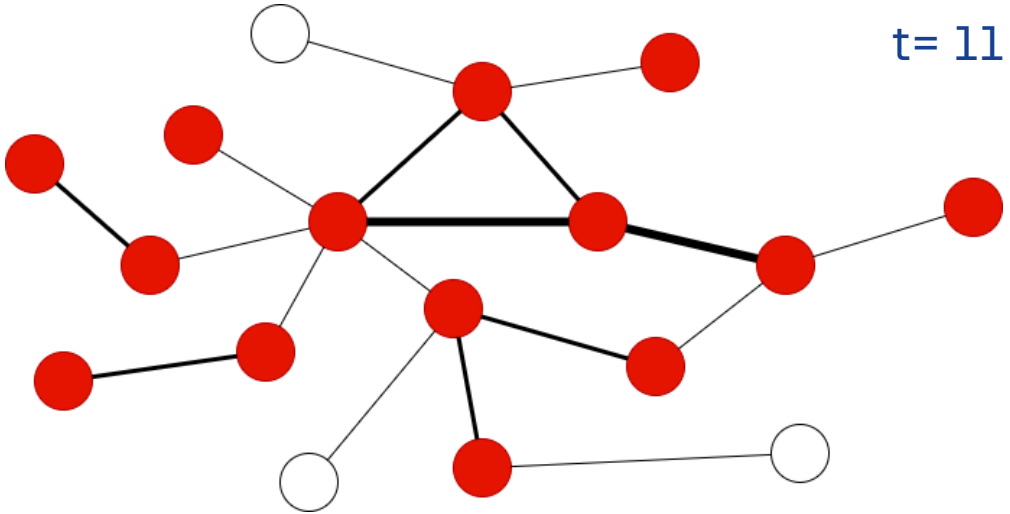
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

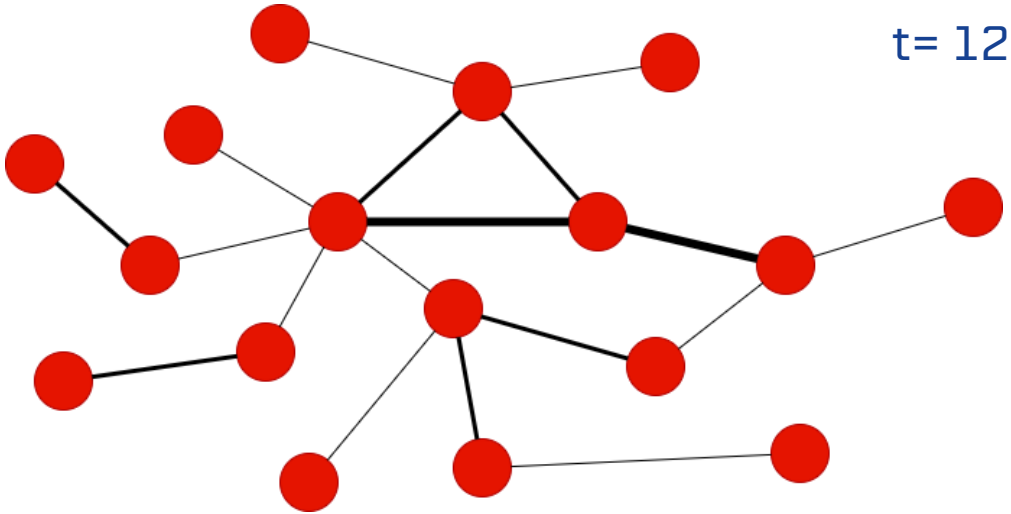
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
   1. La fréquence d'utilisation du lien λ
   2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

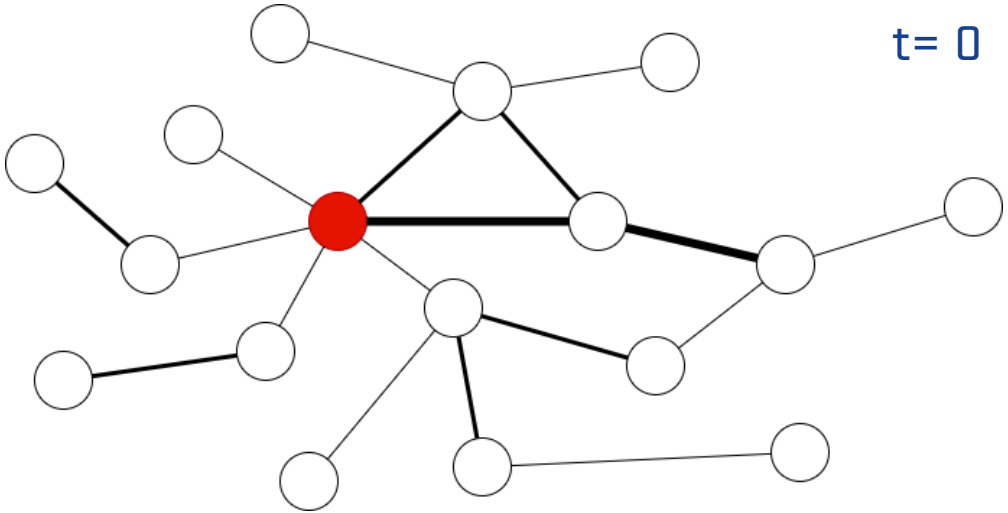
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
   1. La fréquence d'utilisation du lien λ
   2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

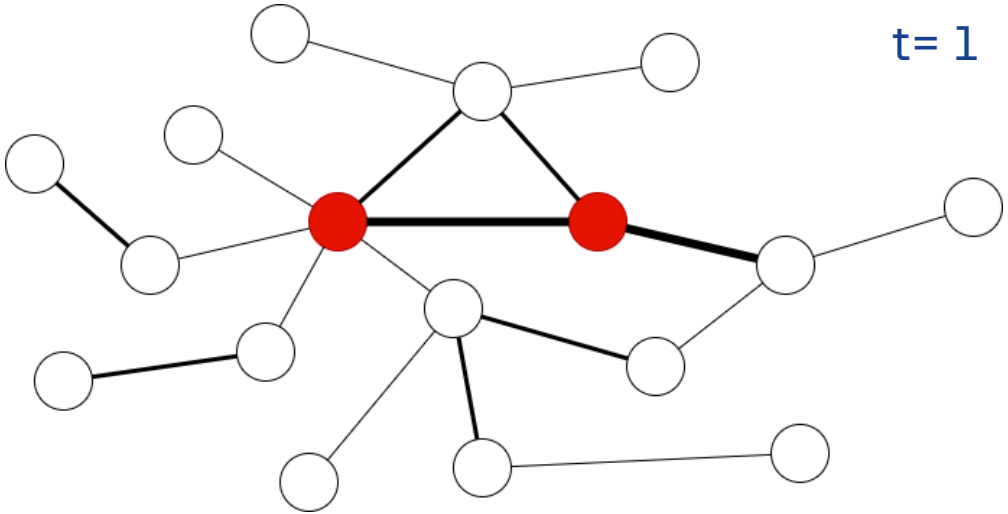
MODÉLISATION DE LA PROPAGATION D'UN MALWARE

1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



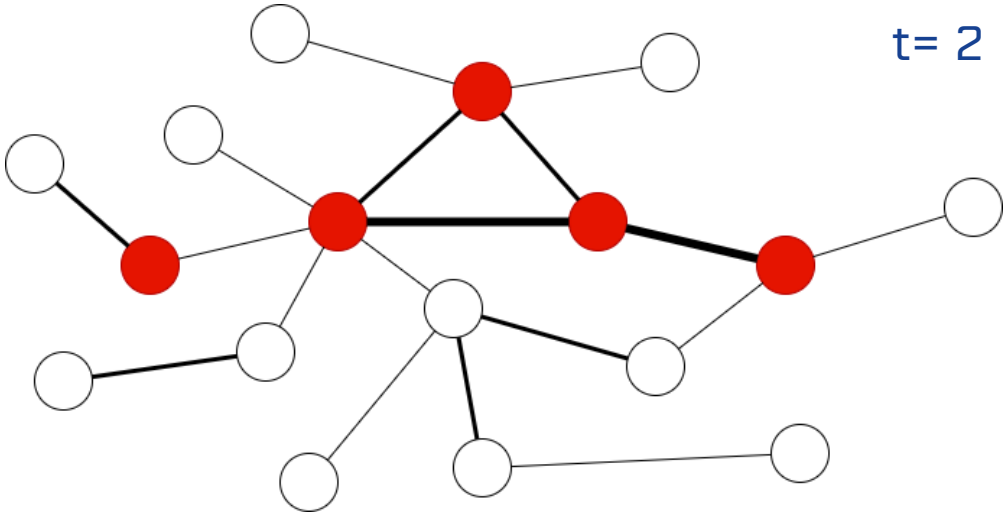
SOLUTIONS EXISTANTES
MODÉLISATION DE LA PROPAGATION D'UN MALWARE

1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES
MODÉLISATION DE LA PROPAGATION D'UN MALWARE

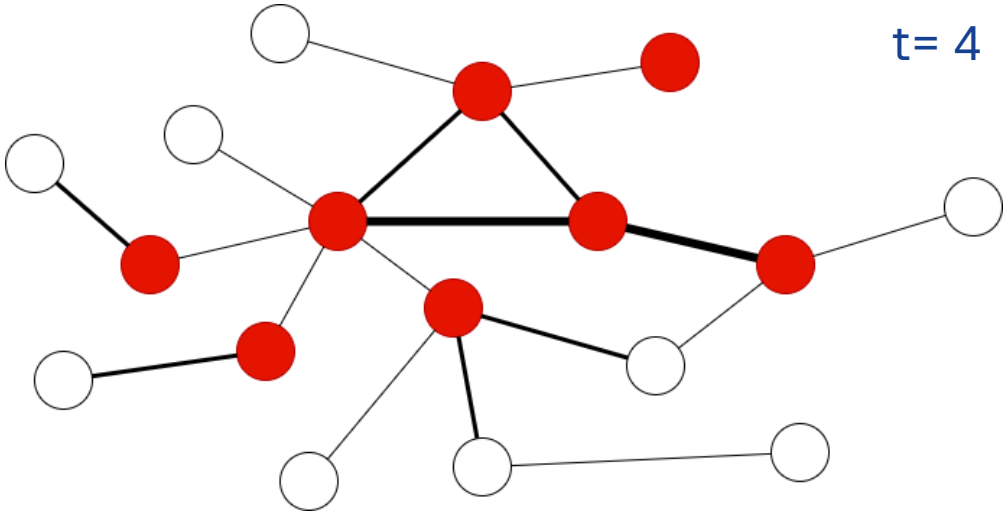
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

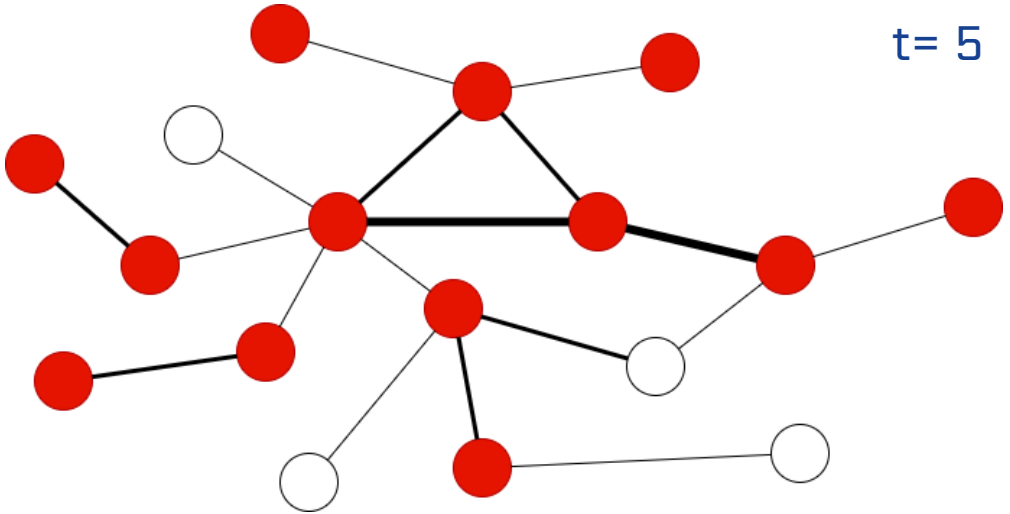
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
    1. La fréquence d'utilisation du lien λ
    2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

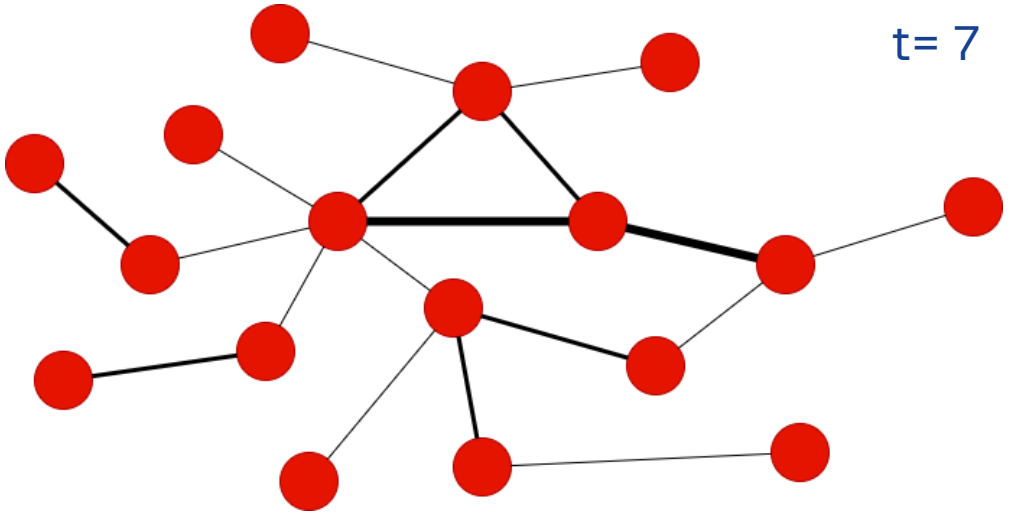
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
   1. La fréquence d'utilisation du lien λ
   2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



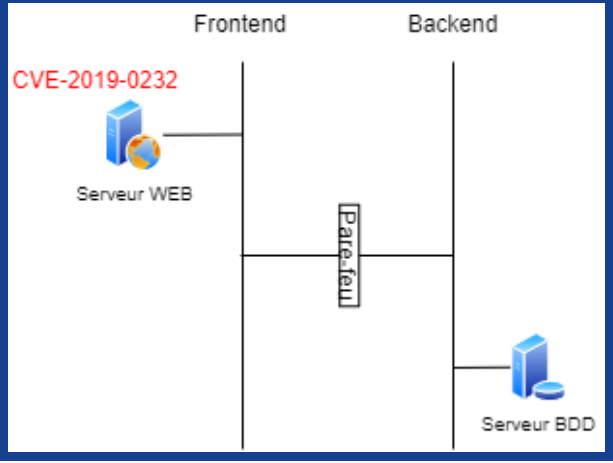
SOLUTIONS EXISTANTES

MODÉLISATION DE LA PROPAGATION D'UN MALWARE

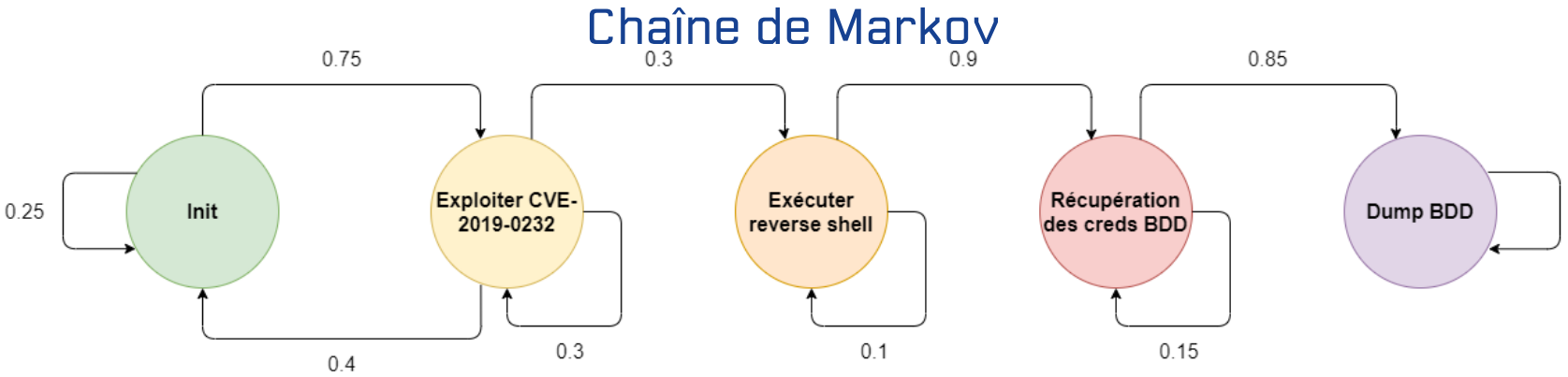
1. Choix du nœud primo-infection
2. Définition pour chaque connexion de :
   1. La fréquence d'utilisation du lien λ
   2. La probabilité de transmission P
3. Propagation du virus au nœud prochain avec une probabilité P
4. Compteur de temps incrémenté en tenant compte du paramètre λ



SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES



SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

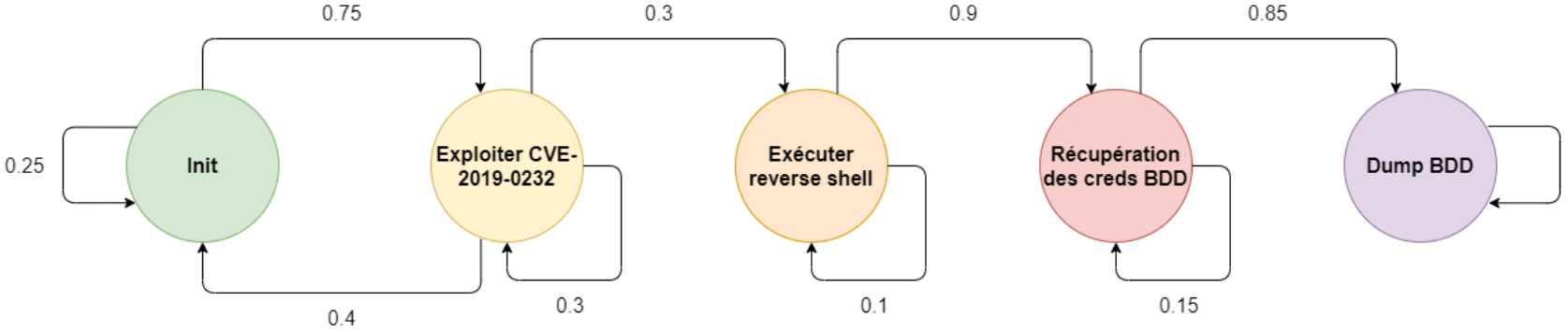


$$S_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad P = \begin{array}{c} \\ From \end{array} \overset{\begin{array}{ccccc} & & To & & \end{array}}{\begin{pmatrix} 0.25 & 0.75 & 0 & 0 & 0 \\ 0.4 & 0.3 & 0.3 & 0 & 0 \\ 0 & 0 & 0.1 & 0.9 & 0 \\ 0 & 0 & 0 & 0.15 & 0.85 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}}$$

SOLUTIONS EXISTANTES

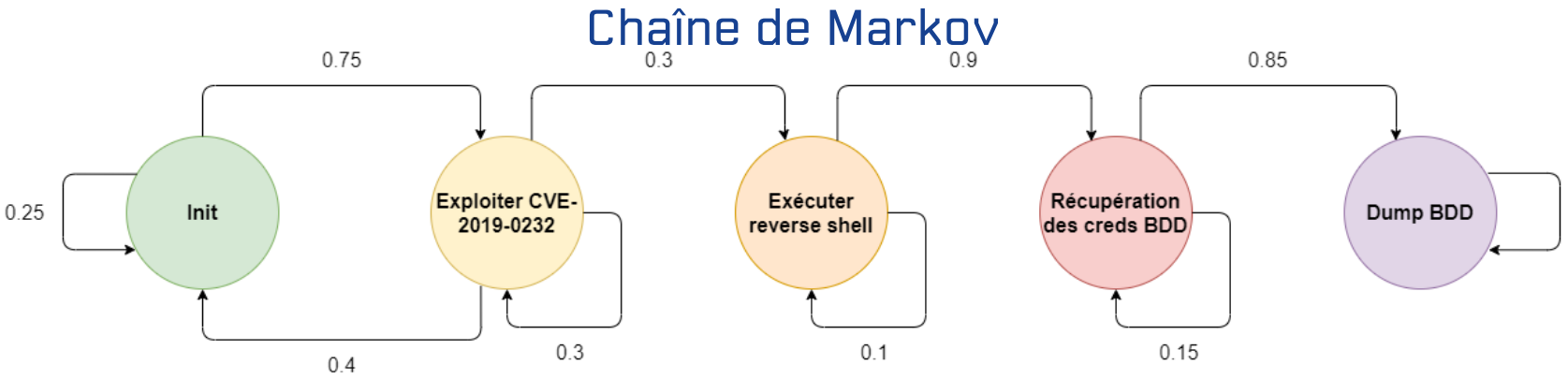
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Chaîne de Markov



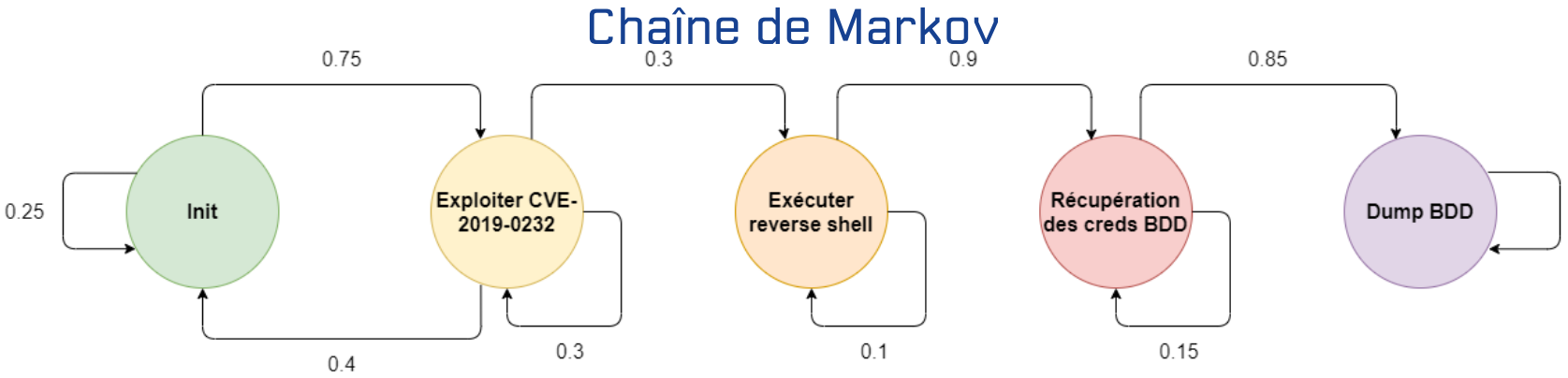
$$S_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0.25 & 0.75 & 0 & 0 & 0 \\ 0.4 & 0.3 & 0.3 & 0 & 0 \\ 0 & 0 & 0.1 & 0.9 & 0 \\ 0 & 0 & 0 & 0.15 & 0.85 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0.25 & 0.75 & 0 & 0 & 0 \end{bmatrix}$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES



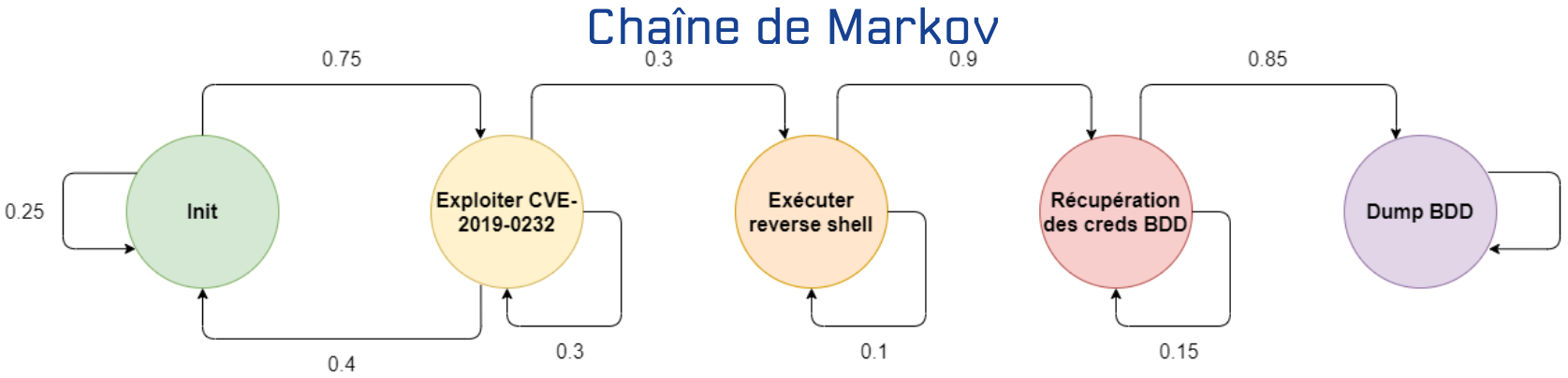
$$S_2 = \begin{bmatrix} 0.25 & 0.75 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0.25 & 0.75 & 0 & 0 & 0 \\ 0.4 & 0.3 & 0.3 & 0 & 0 \\ 0 & 0 & 0.1 & 0.9 & 0 \\ 0 & 0 & 0 & 0.15 & 0.85 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0.36 & 0.41 & 0.23 & 0 & 0 \end{bmatrix}$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES



$$S_3 = \begin{bmatrix} 0.36 & 0.41 & 0.23 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0.25 & 0.75 & 0 & 0 & 0 \\ 0.4 & 0.3 & 0.3 & 0 & 0 \\ 0 & 0 & 0.1 & 0.9 & 0 \\ 0 & 0 & 0 & 0.15 & 0.85 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0.25 & 0.40 & 0.15 & 0.20 & 0 \end{bmatrix}$$

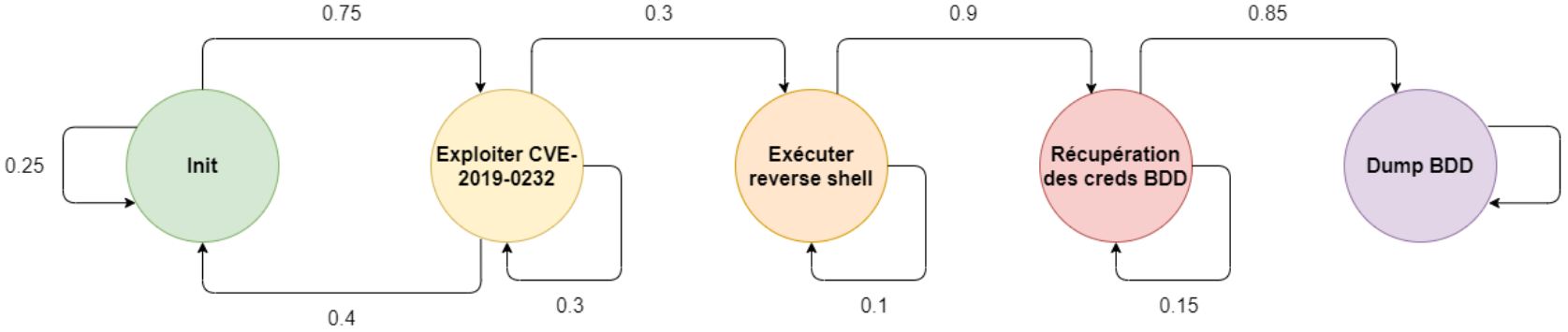
SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES



$$S_4 = \begin{bmatrix} 0.25 & 0.40 & 0.15 & 0.20 & 0 \end{bmatrix} \times \begin{bmatrix} 0.25 & 0.75 & 0 & 0 & 0 \\ 0.4 & 0.3 & 0.3 & 0 & 0 \\ 0 & 0 & 0.1 & 0.9 & 0 \\ 0 & 0 & 0 & 0.15 & 0.85 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0.22 & 0.3 & 0.14 & 0.17 & 0.17 \end{bmatrix}$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Chaîne de Markov



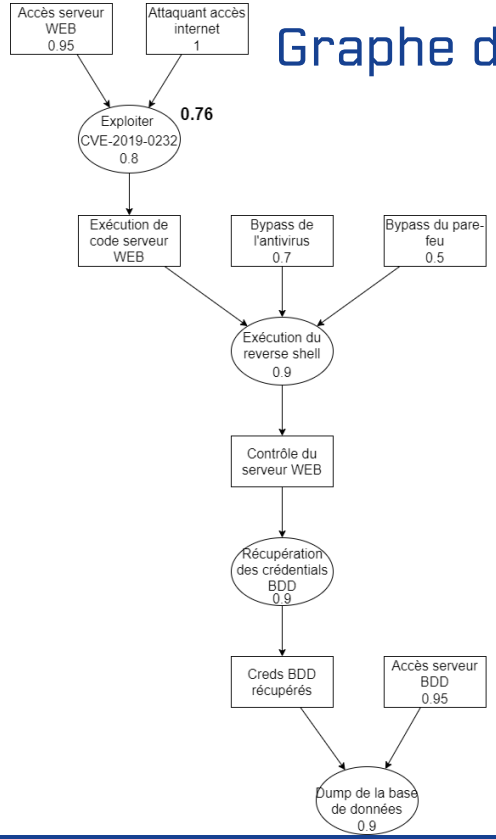
$$S \times P = S$$

$$\Rightarrow \begin{cases} s_0 + s_1 + \cdots + s_n = 1 \\ s_0 * a_{00} + s_1 * a_{10} + \cdots + s_n * a_{n0} = s_0 \\ s_0 * a_{01} + s_1 * a_{11} + \cdots + s_n * a_{n1} = s_1 \\ \vdots \\ s_0 * a_{0n} + s_1 * a_{1n} + \cdots + s_n * a_{nn} = s_n \end{cases}$$

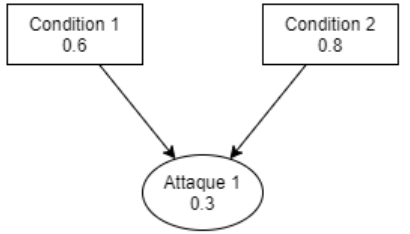
$$S_{stable} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Graphe d'attaques

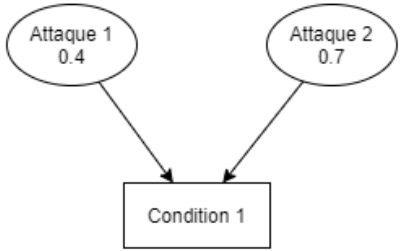


Règles de calculs



$$P(\bigcap_{i=0}^{n} X_i) = \prod_{i=0}^{n} P(X_i)$$

$$P(Condition1 \bigcap Condition2 \bigcap Attaque1) = 0.6 \times 0.8 \times 0.3 = 0.144$$

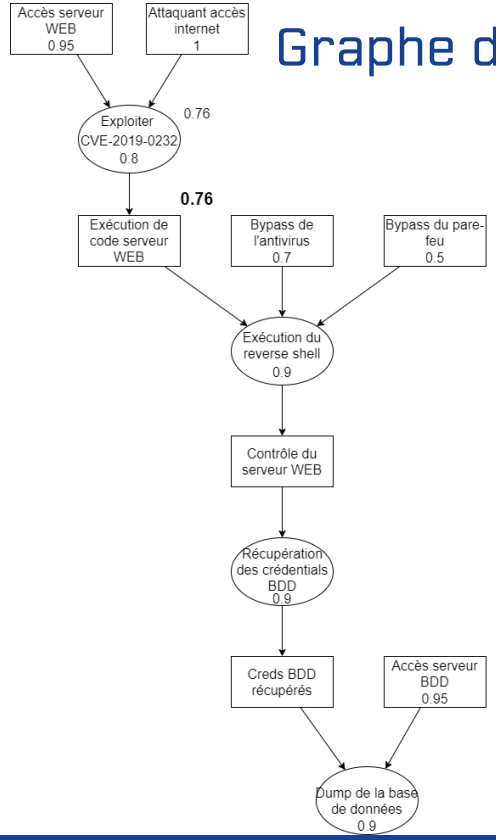


$$P(\bigcup_{i=0}^{n} X_i) = 1 - \prod_{i=0}^{n} P(\overline{X_i})$$

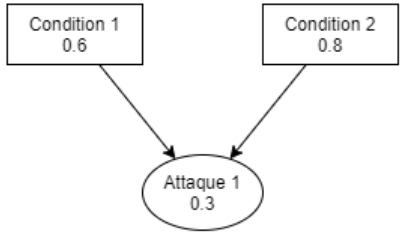
$$P(Attaque1 \bigcup Attaque2) = 1 - 0.6 \times 0.3 = 0.82$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Graphe d'attaques

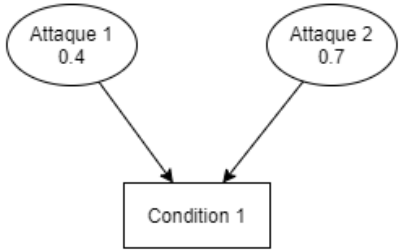


Règles de calculs



$$P(\bigcap_{i=0}^{n} X_i) = \prod_{i=0}^{n} P(X_i)$$

$$P(Condition1 \bigcap Condition2 \bigcap Attaque1) = 0.6 \times 0.8 \times 0.3 = 0.144$$

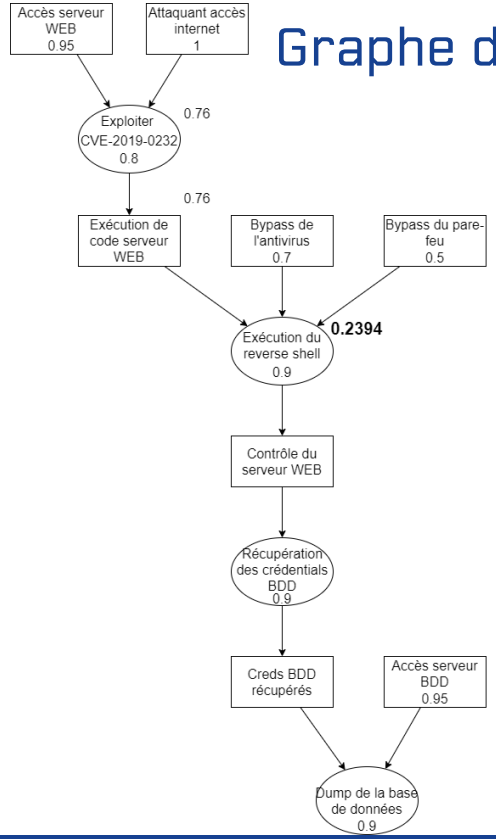


$$P(\bigcup_{i=0}^{n} X_i) = 1 - \prod_{i=0}^{n} P(\overline{X_i})$$

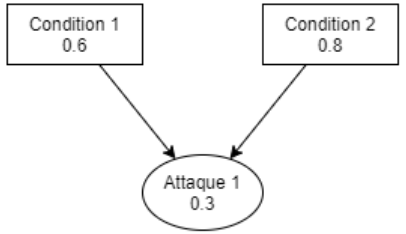
$$P(Attaque1 \bigcup Attaque2) = 1 - 0.6 \times 0.3 = 0.82$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Graphe d'attaques

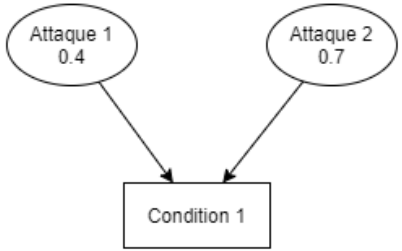


Règles de calculs



$$P(\bigcap_{i=0}^{n} X_i) = \prod_{i=0}^{n} P(X_i)$$

$$P(Condition1 \bigcap Condition2 \bigcap Attaque1) = 0.6 \times 0.8 \times 0.3 = 0.144$$

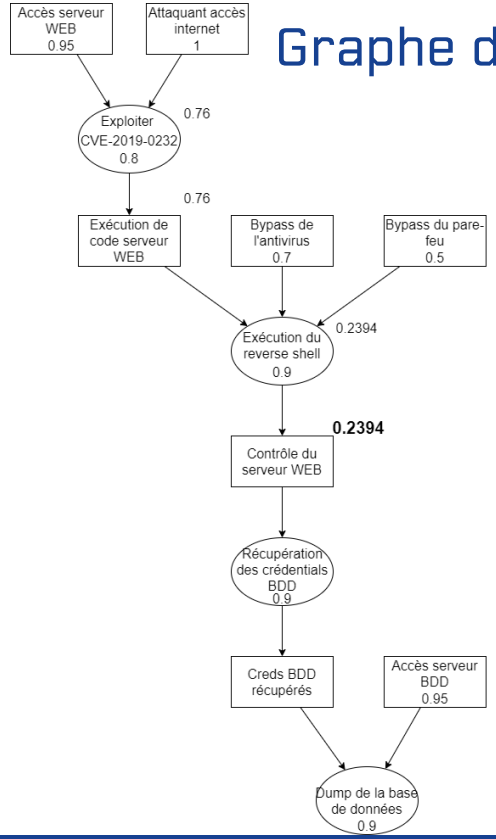


$$P(\bigcup_{i=0}^{n} X_i) = 1 - \prod_{i=0}^{n} P(\overline{X_i})$$

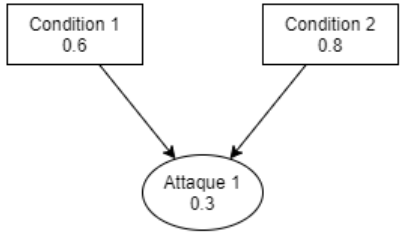
$$P(Attaque1 \bigcup Attaque2) = 1 - 0.6 \times 0.3 = 0.82$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Graphe d'attaques

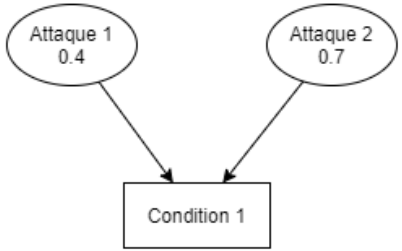


Règles de calculs



$$P(\bigcap_{i=0}^{n} X_i) = \prod_{i=0}^{n} P(X_i)$$

$$P(Condition1 \bigcap Condition2 \bigcap Attaque1) = 0.6 \times 0.8 \times 0.3 = 0.144$$

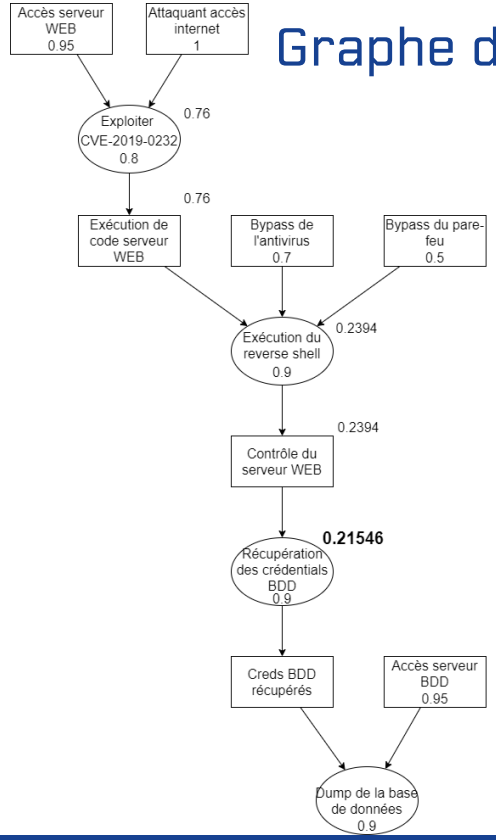


$$P(\bigcup_{i=0}^{n} X_i) = 1 - \prod_{i=0}^{n} P(\overline{X_i})$$

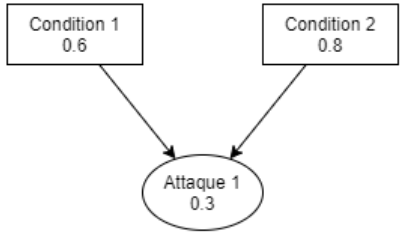
$$P(Attaque1 \bigcup Attaque2) = 1 - 0.6 \times 0.3 = 0.82$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Graphe d'attaques

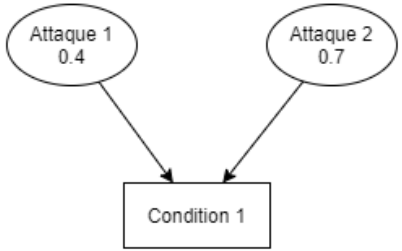


Règles de calculs



$$P(\bigcap_{i=0}^{n} X_i) = \prod_{i=0}^{n} P(X_i)$$

$$P(Condition1 \bigcap Condition2 \bigcap Attaque1) = 0.6 \times 0.8 \times 0.3 = 0.144$$

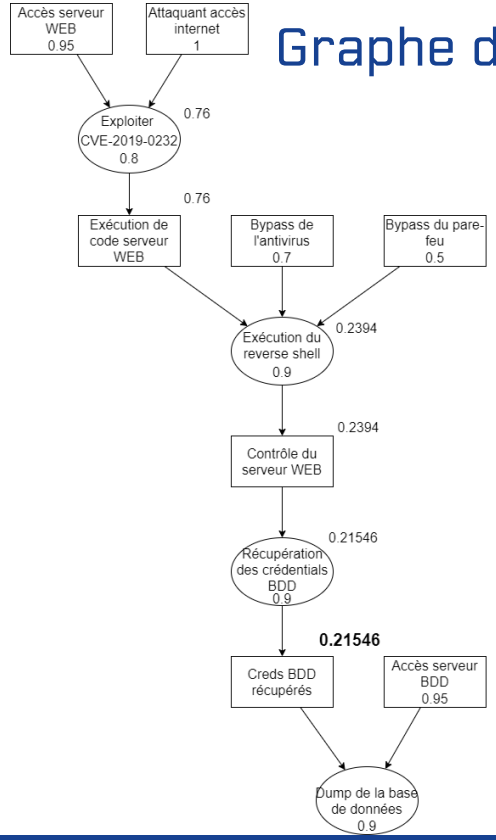


$$P(\bigcup_{i=0}^{n} X_i) = 1 - \prod_{i=0}^{n} P(\overline{X_i})$$

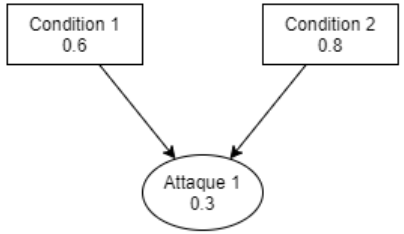
$$P(Attaque1 \bigcup Attaque2) = 1 - 0.6 \times 0.3 = 0.82$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Graphe d'attaques

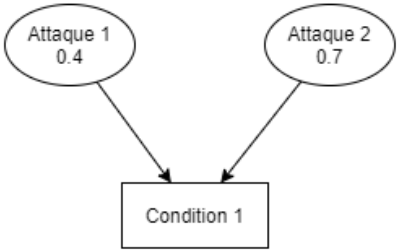


Règles de calculs



$$P(\bigcap_{i=0}^{n} X_i) = \prod_{i=0}^{n} P(X_i)$$

$$P(Condition1 \bigcap Condition2 \bigcap Attaque1) = 0.6 \times 0.8 \times 0.3 = 0.144$$

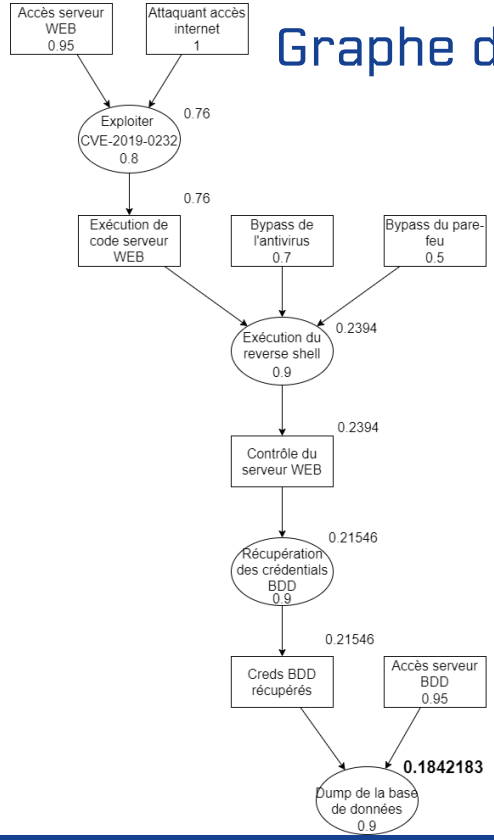


$$P(\bigcup_{i=0}^{n} X_i) = 1 - \prod_{i=0}^{n} P(\overline{X_i})$$

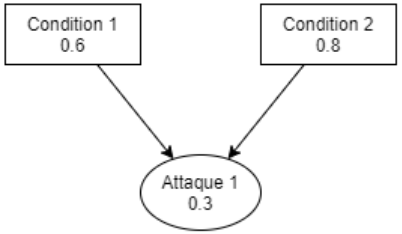
$$P(Attaque1 \bigcup Attaque2) = 1 - 0.6 \times 0.3 = 0.82$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Graphe d'attaques

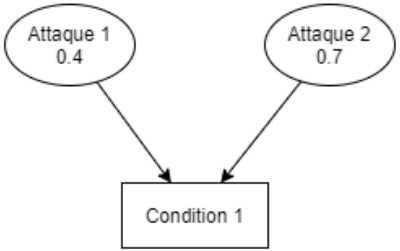


Règles de calculs



$$P(\bigcap_{i=0}^{n} X_i) = \prod_{i=0}^{n} P(X_i)$$

$$P(Condition1 \bigcap Condition2 \bigcap Attaque1) = 0.6 \times 0.8 \times 0.3 = 0.144$$

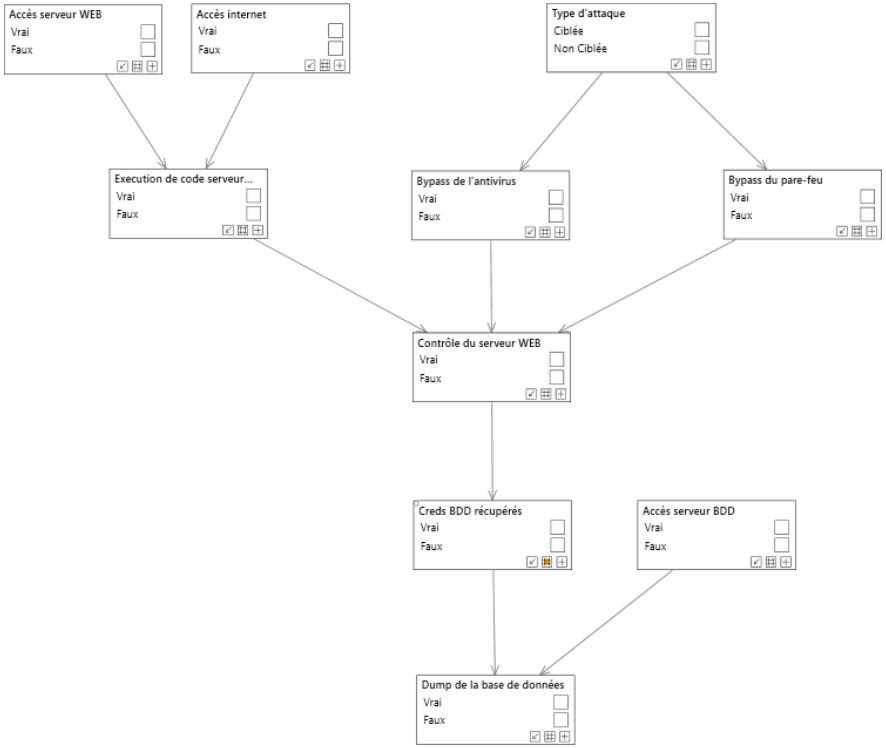


$$P(\bigcup_{i=0}^{n} X_i) = 1 - \prod_{i=0}^{n} P(\overline{X_i})$$

$$P(Attaque1 \bigcup Attaque2) = 1 - 0.6 \times 0.3 = 0.82$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Réseaux Bayésiens



Tables de probabilités conditionnelles

Type d'attaque	Bypass de l'antivirus = Vrai	Bypass de l'antivirus = Faux
Ciblée	0,8	0,2
Non Ciblée	0,15	0,85

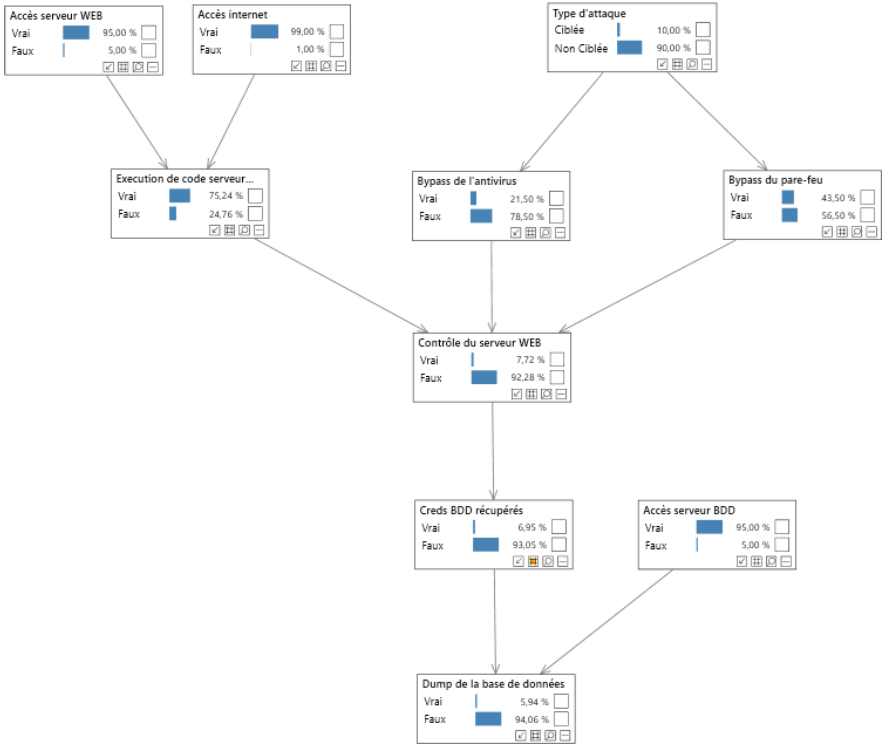
Nœud Bypass antivirus

Creds BDD récupérés	Accès serveur BDD	Dump BDD = Vrai	Dump BDD = Faux
Vrai	Vrai	0,9	0,1
Vrai	Faux	0	1
Faux	Vrai	0	1
Faux	Faux	0	1

Nœud Dump BDD

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Réseaux Bayésiens



Règles de calculs

$P(X_i|PARENTS(Xi))$

Creds BDD récupérés	Accès serveur BDD	Dump BDD = Vrai	Dump BDD = Faux
Vrai	Vrai	0,9	0,1
Vrai	Faux	0	1
Faux	Vrai	0	1
Faux	Faux	0	1

Probabilités conditionnelles

$$P(X_1, X_2, ..., X_n) = \prod_{i=1}^{n} P(X_i|PARENTS(X_i))$$

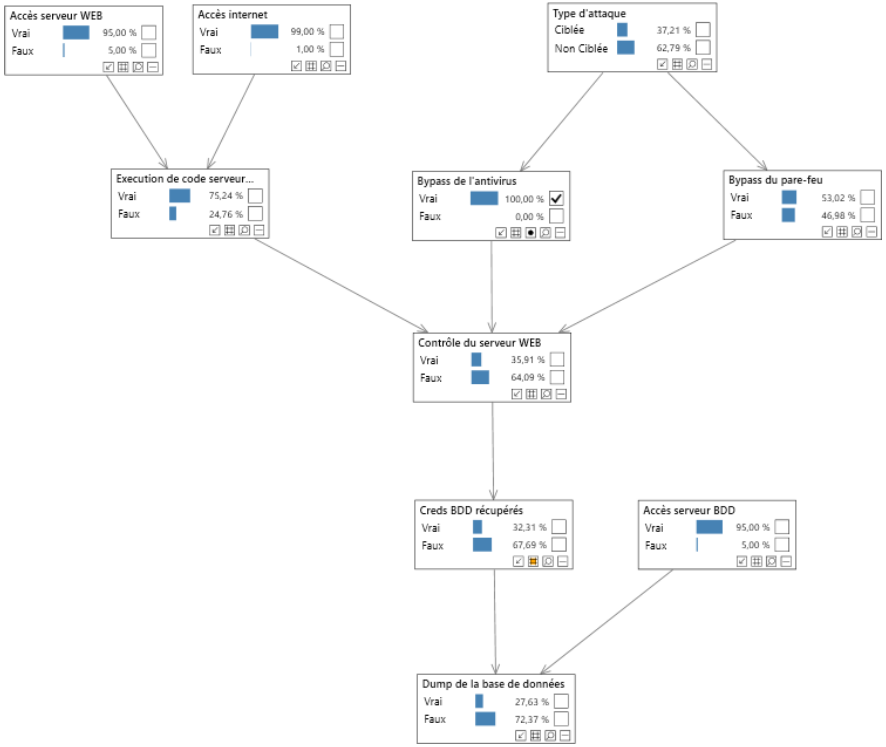
Probabilités conjointes

$$P(X_i = x) = \sum_{X_1} ... \sum_{X_{i-1}} \sum_{X_{i+1}} ... \sum_{X_n} P(X1, ..., X_i = x, ..., X_n)$$

Probabilités marginales

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Réseaux Bayésiens



Règles de calculs

$$P(X_i = x | E = e) = \frac{P(X_i = x, E = e)}{P(E = e)}$$

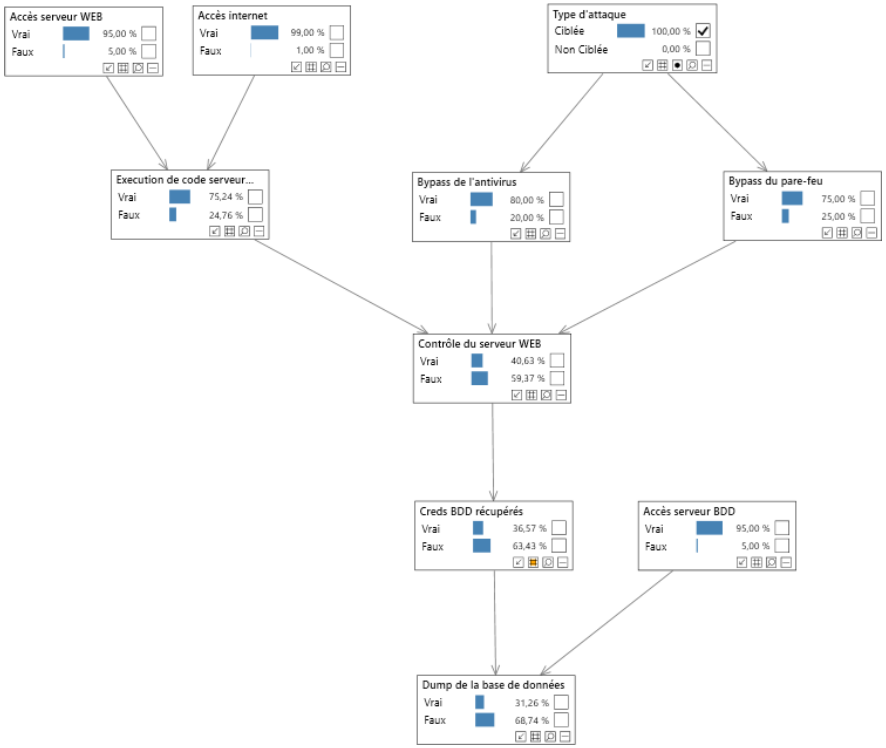
avec,

$$P(X_i = x, E = e) = \sum_Y P(X_i = x, Y, E = e)$$

$$P(E = e) = \sum_X \sum_Y P(X, Y, E = e)$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Réseaux Bayésiens



Règles de calculs

$$P(X_i = x | E = e) = \frac{P(X_i = x, E = e)}{P(E = e)}$$

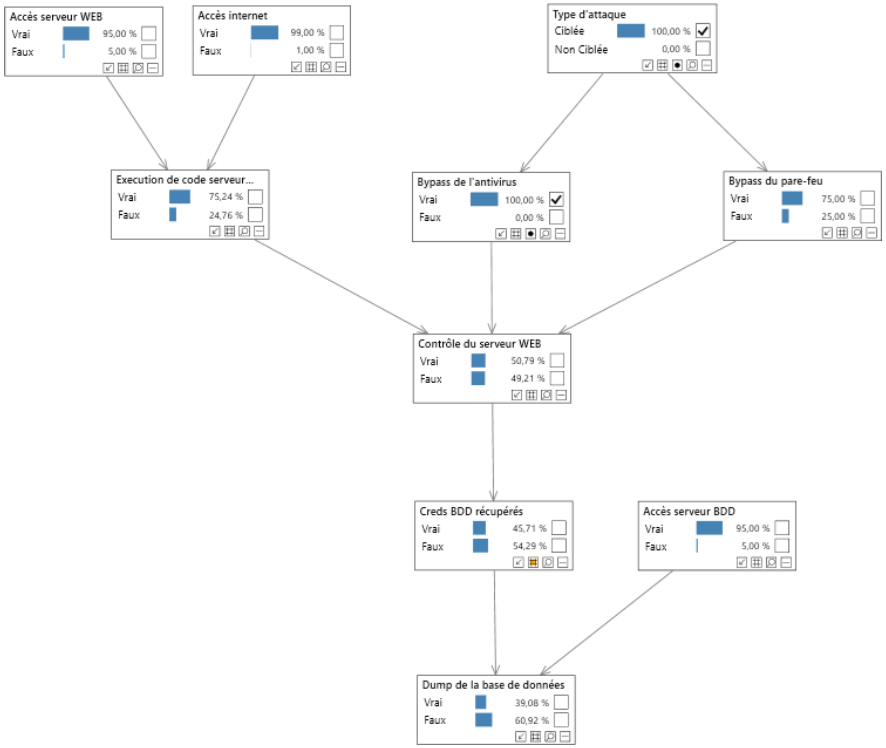
avec,

$$P(X_i = x, E = e) = \sum_Y P(X_i = x, Y, E = e)$$

$$P(E = e) = \sum_X \sum_Y P(X, Y, E = e)$$

SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Réseaux Bayésiens



Règles de calculs

$$P(X_i = x | E = e) = \frac{P(X_i = x, E = e)}{P(E = e)}$$

avec,

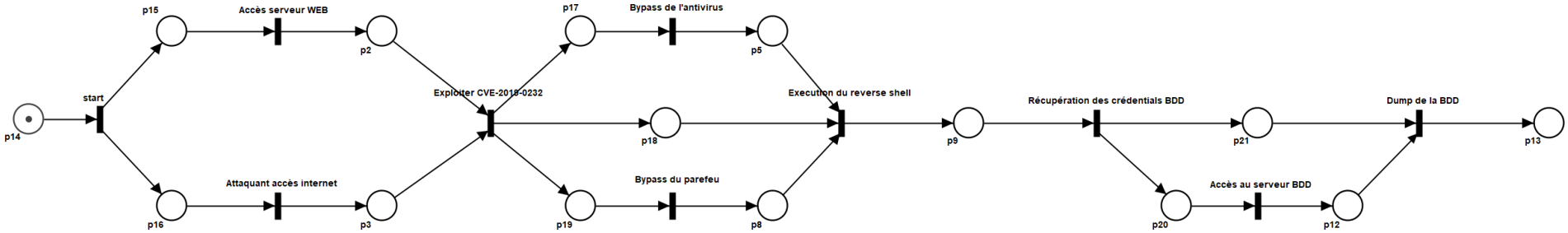
$$P(X_i = x, E = e) = \sum_Y P(X_i = x, Y, E = e)$$

$$P(E = e) = \sum_X \sum_Y P(X, Y, E = e)$$

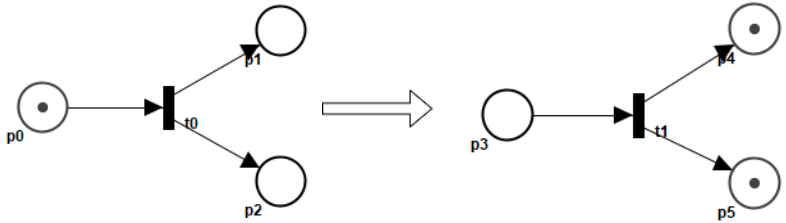
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

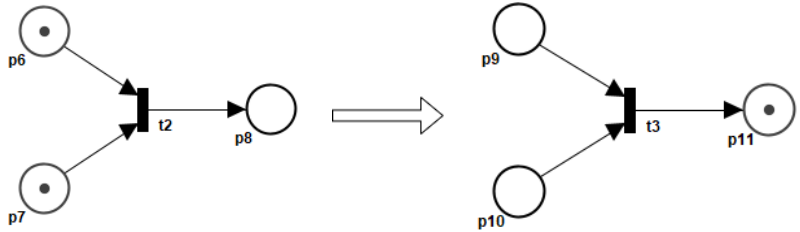
Réseau de Pétri



Règle 1



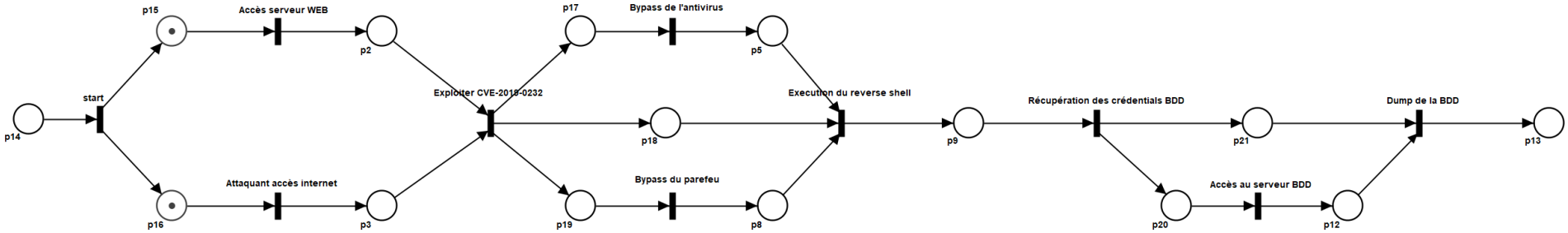
Règle 2



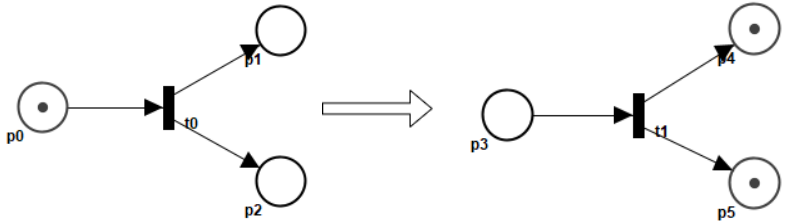
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

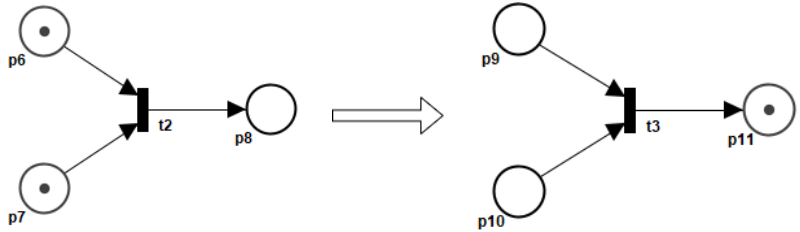
Réseau de Pétri



Règle 1



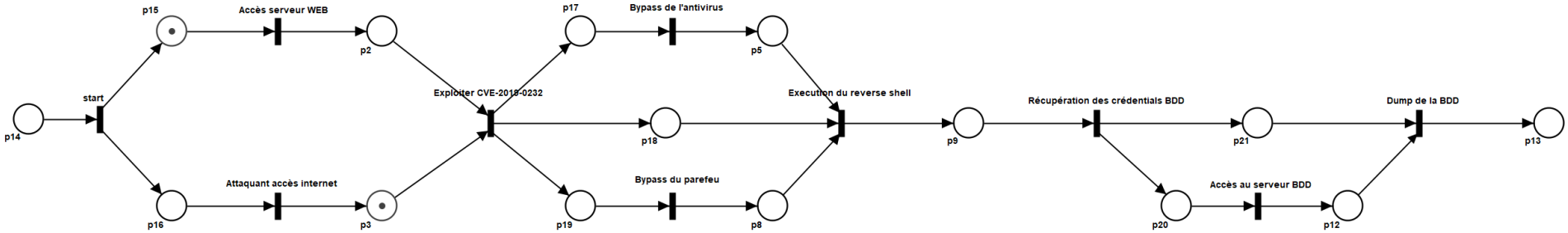
Règle 2



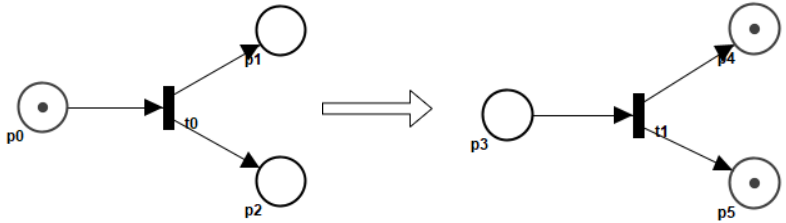
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

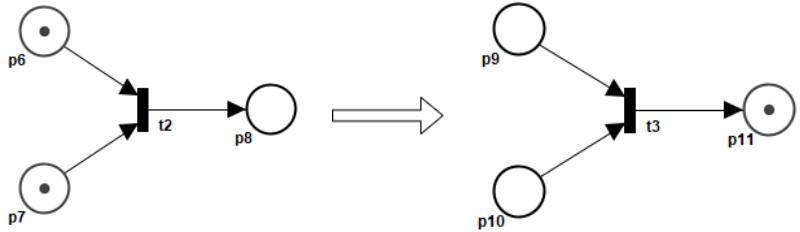
Réseau de Pétri



Règle 1



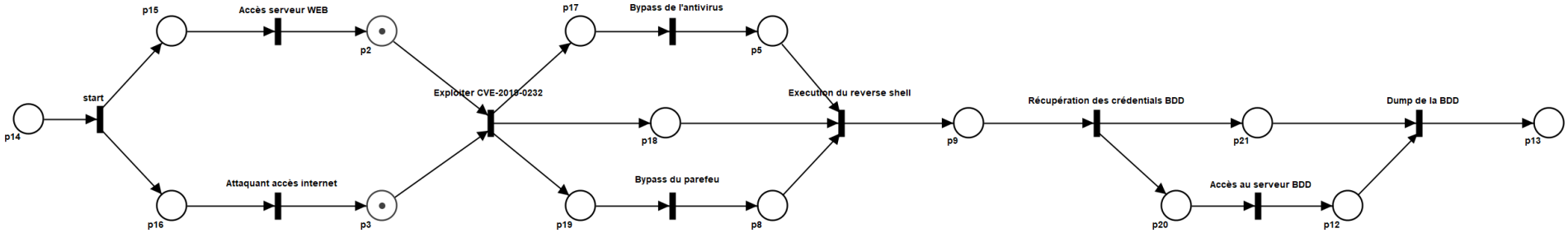
Règle 2



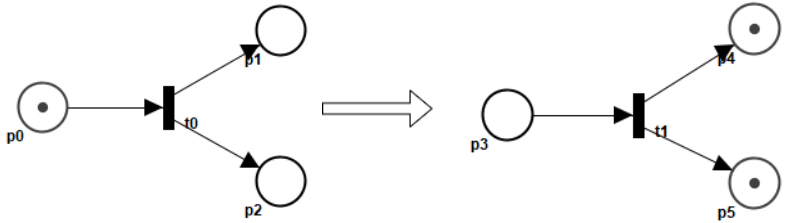
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

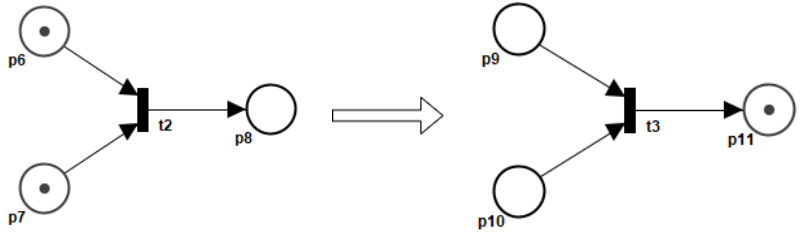
Réseau de Pétri



Règle 1

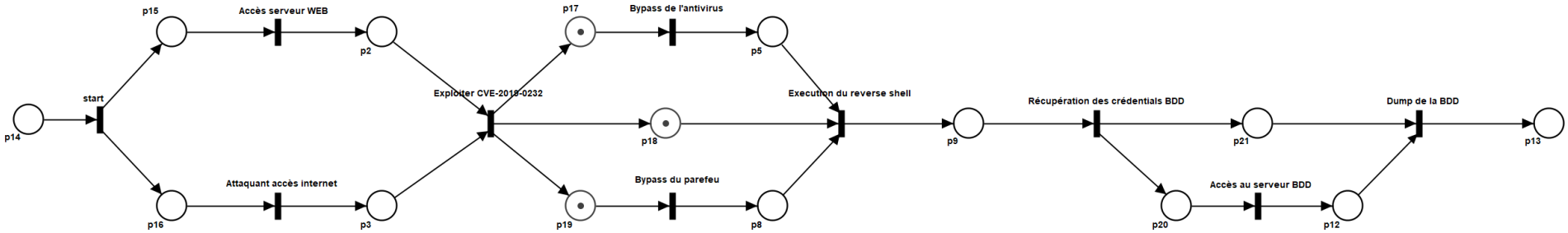


Règle 2

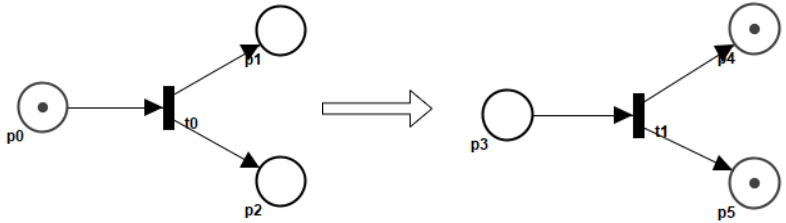


SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

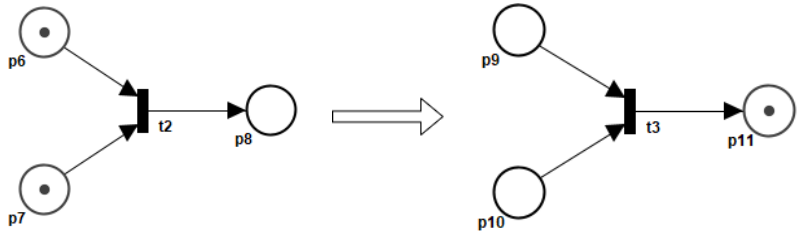
Réseau de Pétri



Règle 1



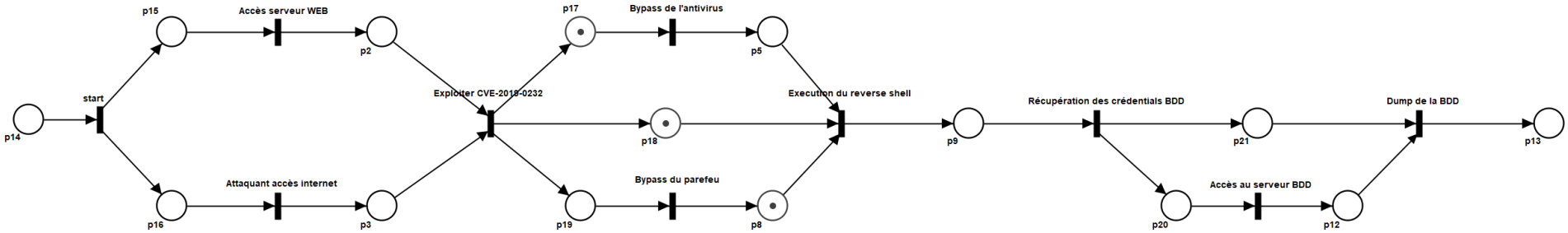
Règle 2



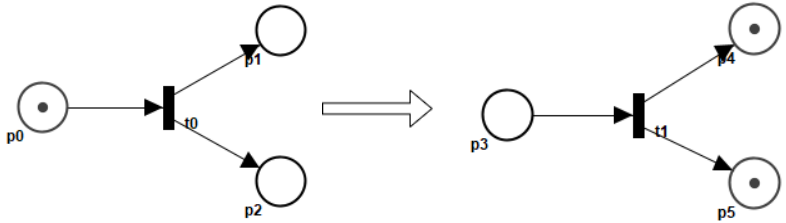
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

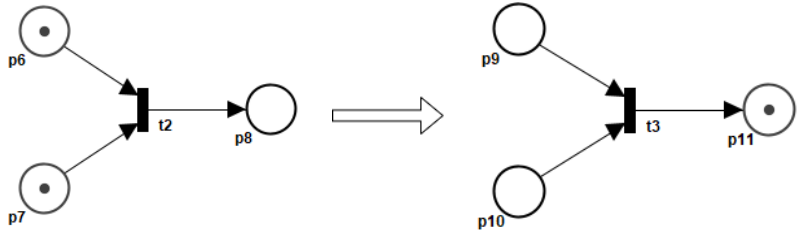
Réseau de Pétri



Règle 1

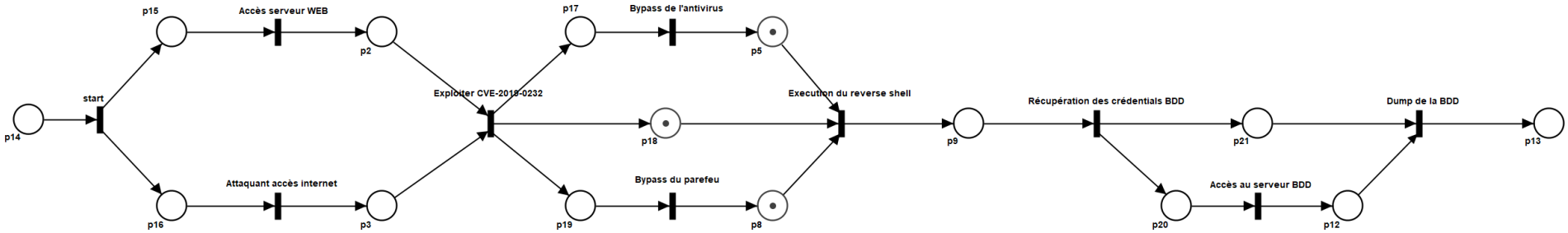


Règle 2

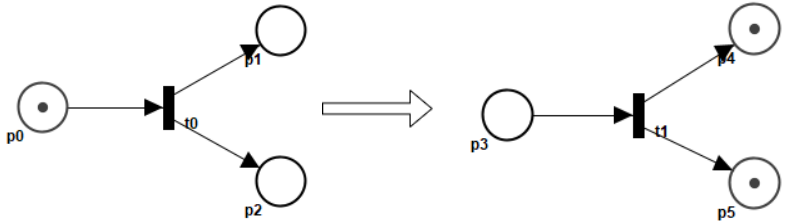


SOLUTIONS EXISTANTES
MODÉLISATION DE SCÉNARIOS D'ATTAQUES

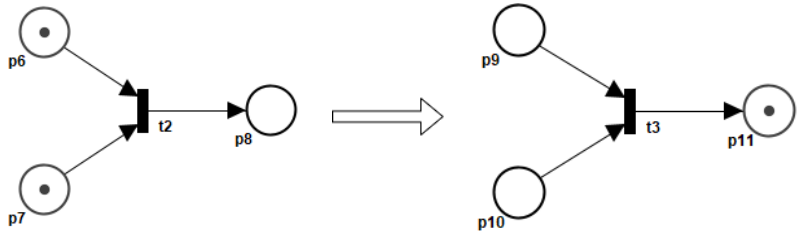
Réseau de Pétri



Règle 1



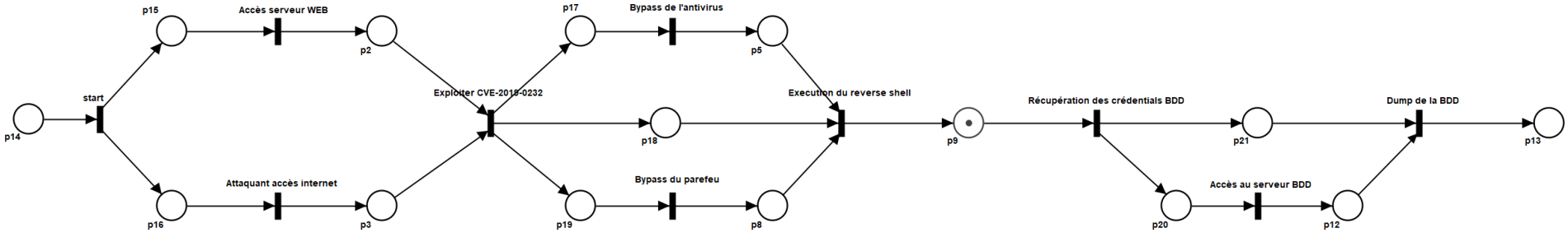
Règle 2



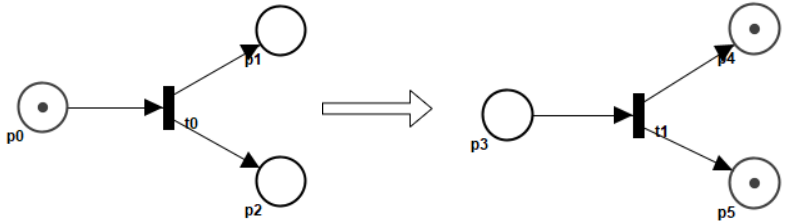
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

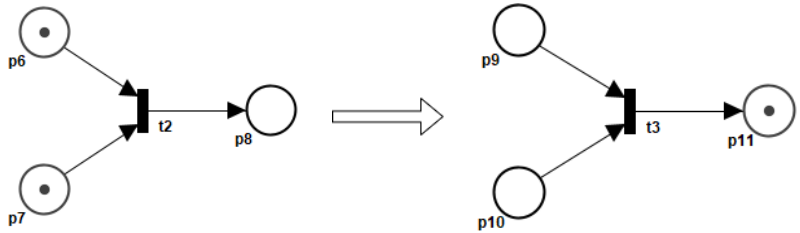
Réseau de Pétri



Règle 1



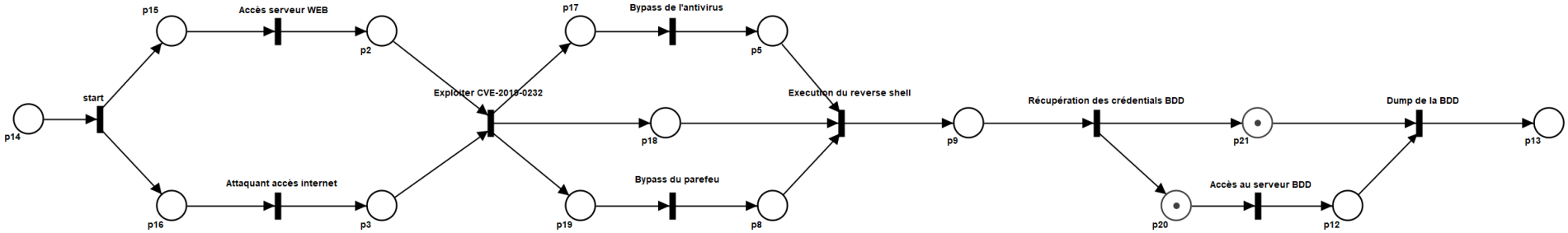
Règle 2



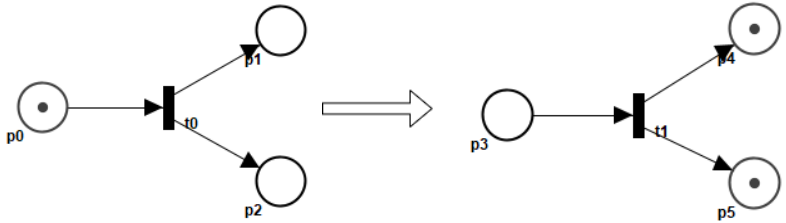
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

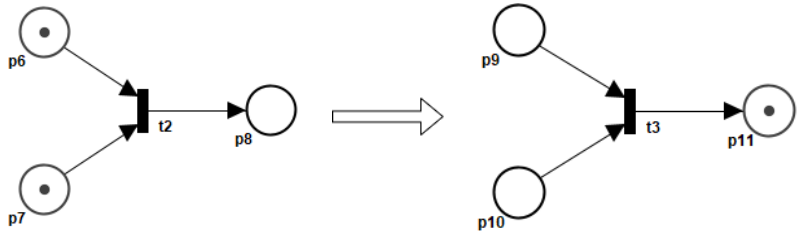
Réseau de Pétri



Règle 1



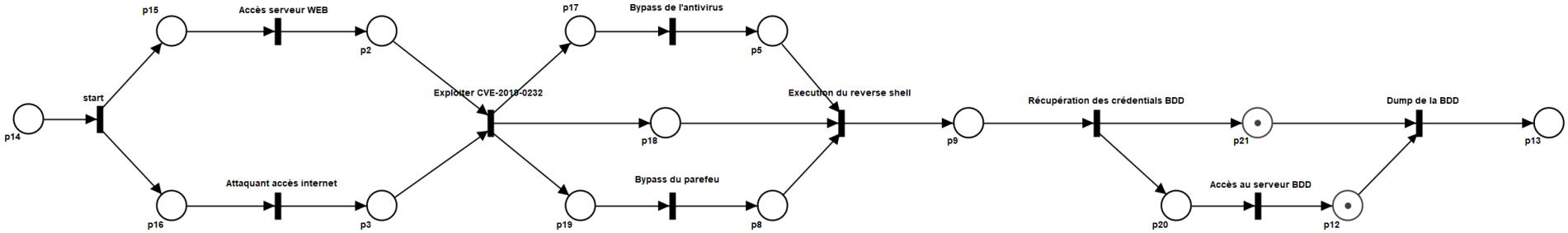
Règle 2



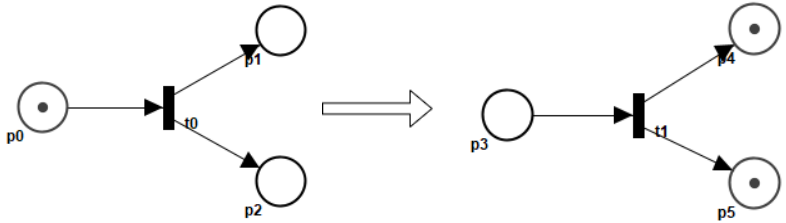
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

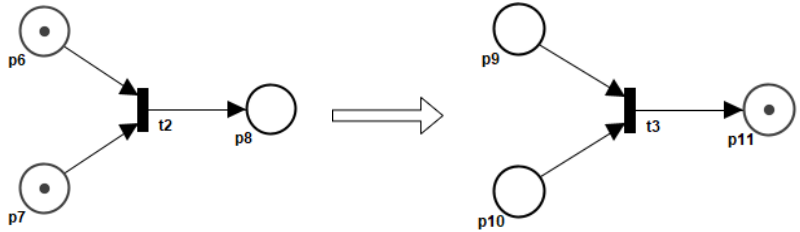
Réseau de Pétri



Règle 1



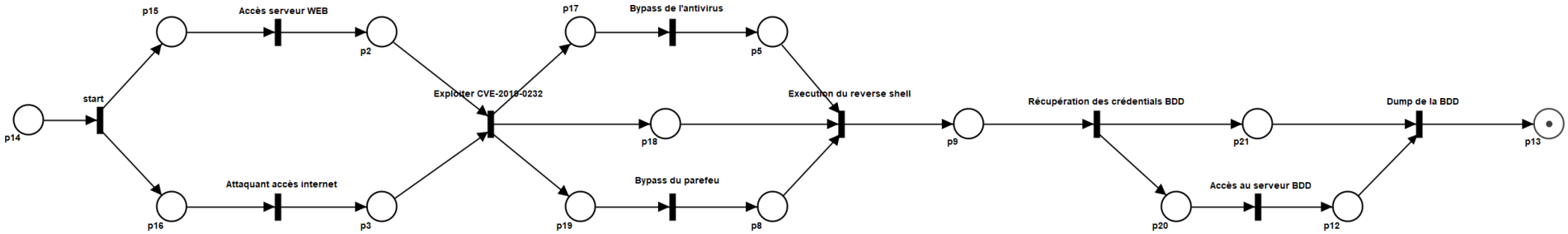
Règle 2



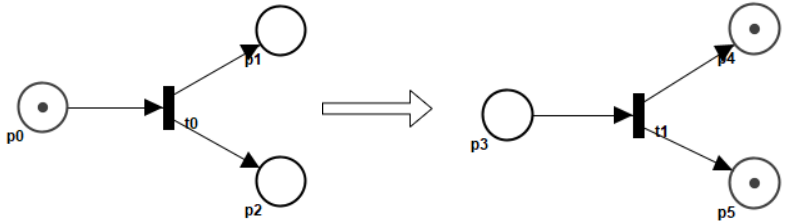
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

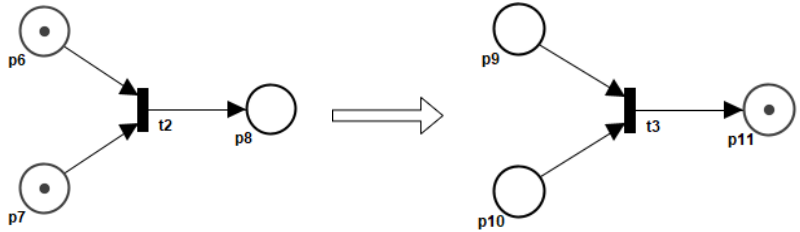
Réseau de Pétri



Règle 1



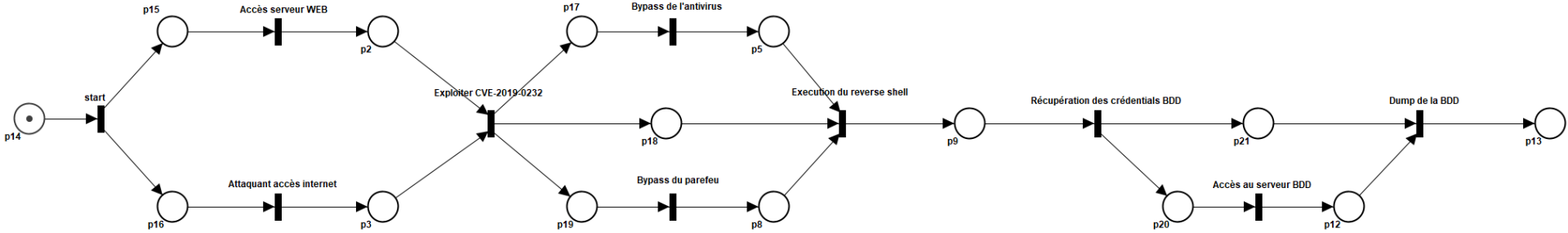
Règle 2



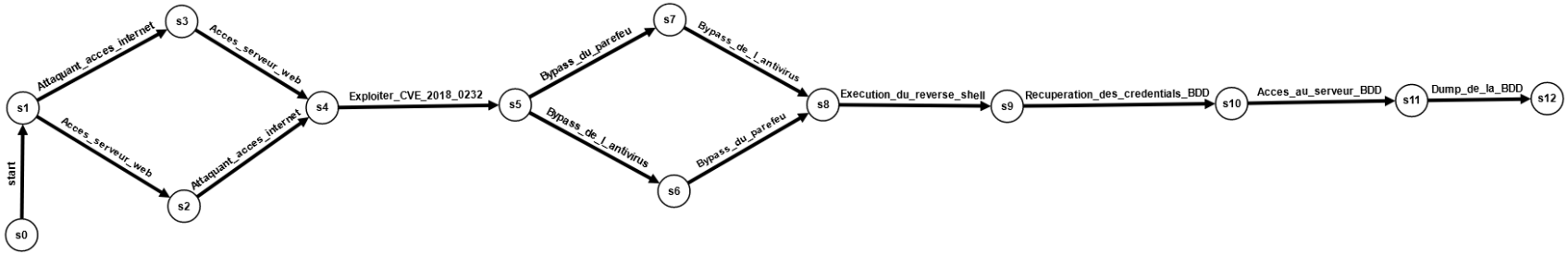
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Réseau de Pétri



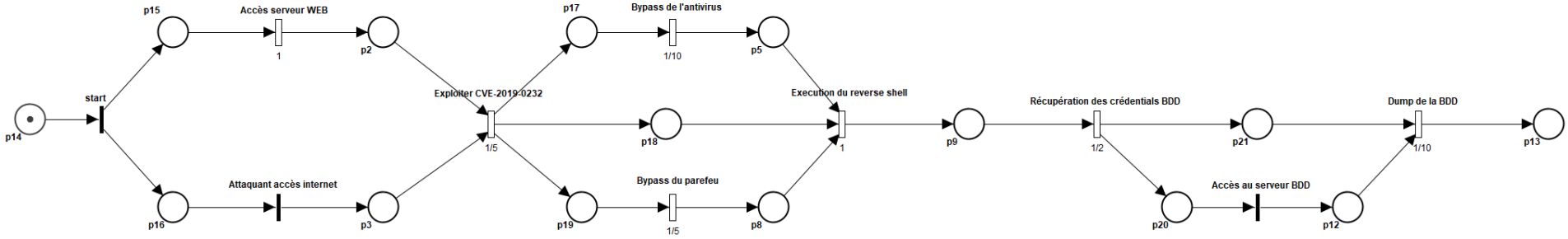
Graphe d'accessibilité



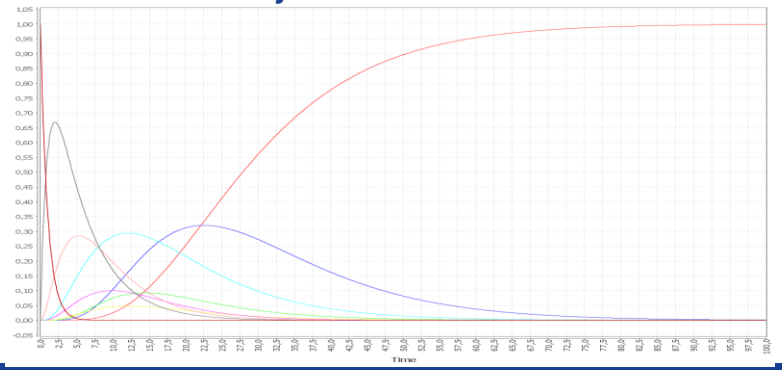
SOLUTIONS EXISTANTES

MODÉLISATION DE SCÉNARIOS D'ATTAQUES

Réseau de Pétri



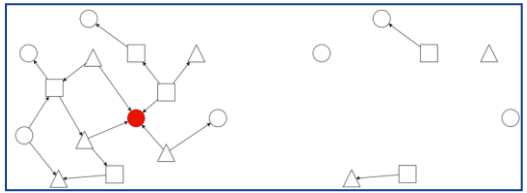
Analyse transitoire

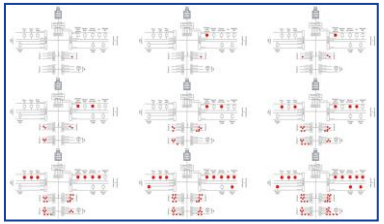


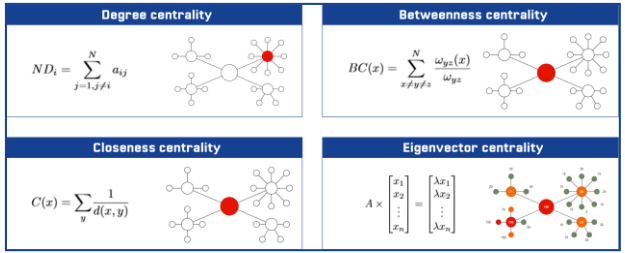
CONCLUSION

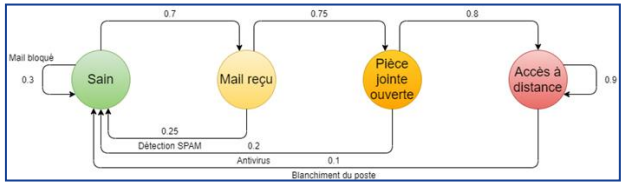
CONCLUSION

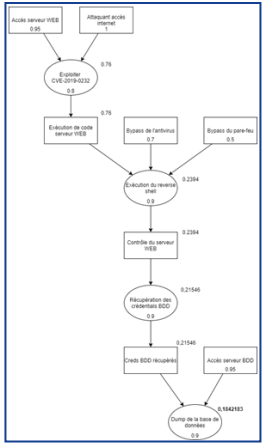
Polynomiale



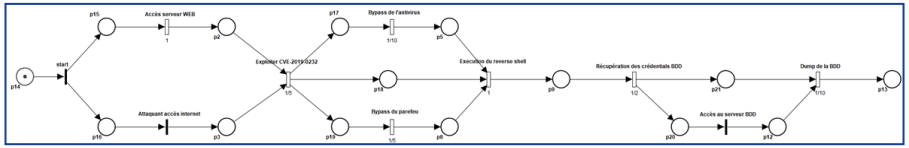


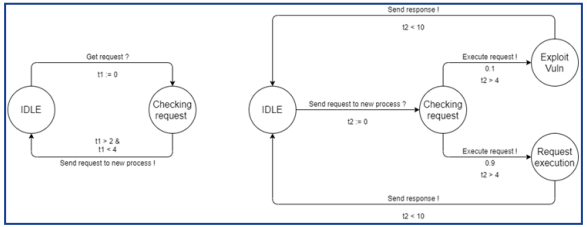


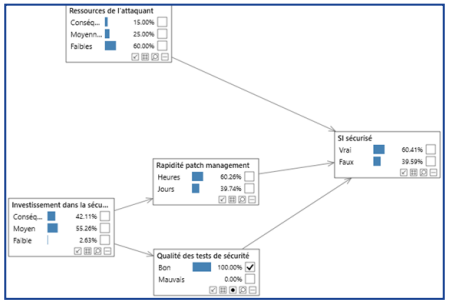




Non polynomiale







CONCLUSION

Est ce que la problématique est résolue ?

Il existe des modèles permettant de calculer la probabilité d'exploitation et l'impact de la vulnérabilité sur le système.

Mais il existe encore des limitations :

- Temps de calcul importants.
- Difficulté à générer les modèles.
- Limitations aux CVE et CVSS.

QUESTIONS