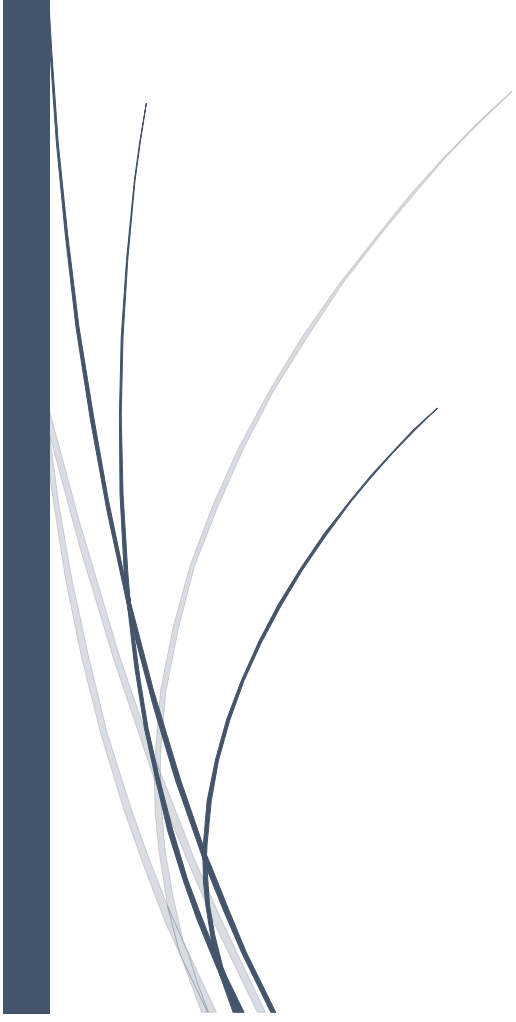
21/11/2016

Threat and risk analysis, IT security audit and norms



Aurélien Monnet-Paquet
UGA – MASTER 2 CYBERSECURITY

Threat and risk analysis, IT security audit and norms

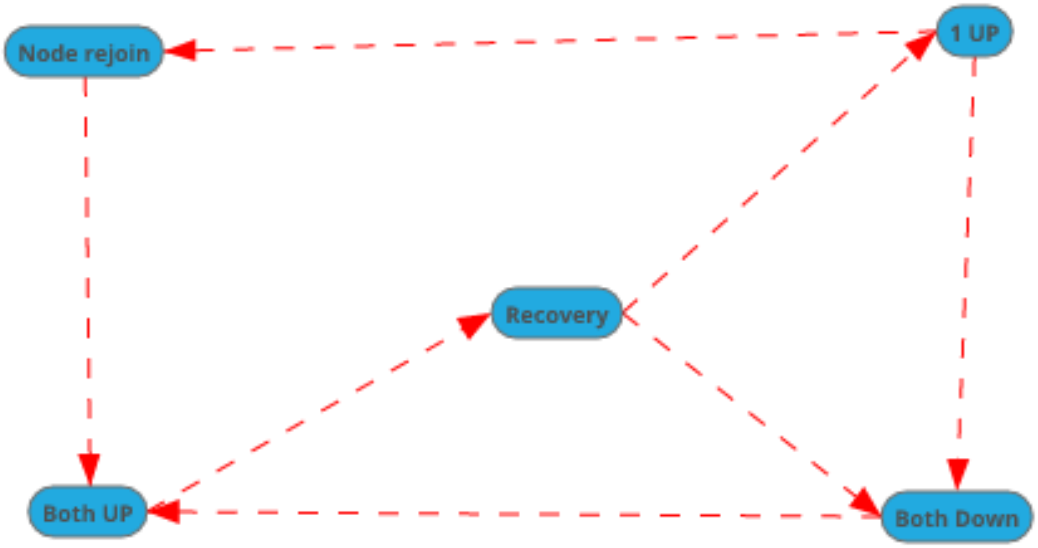
Par Aurélien Monnet-Paquet.

Ex 1

Différents états possible :

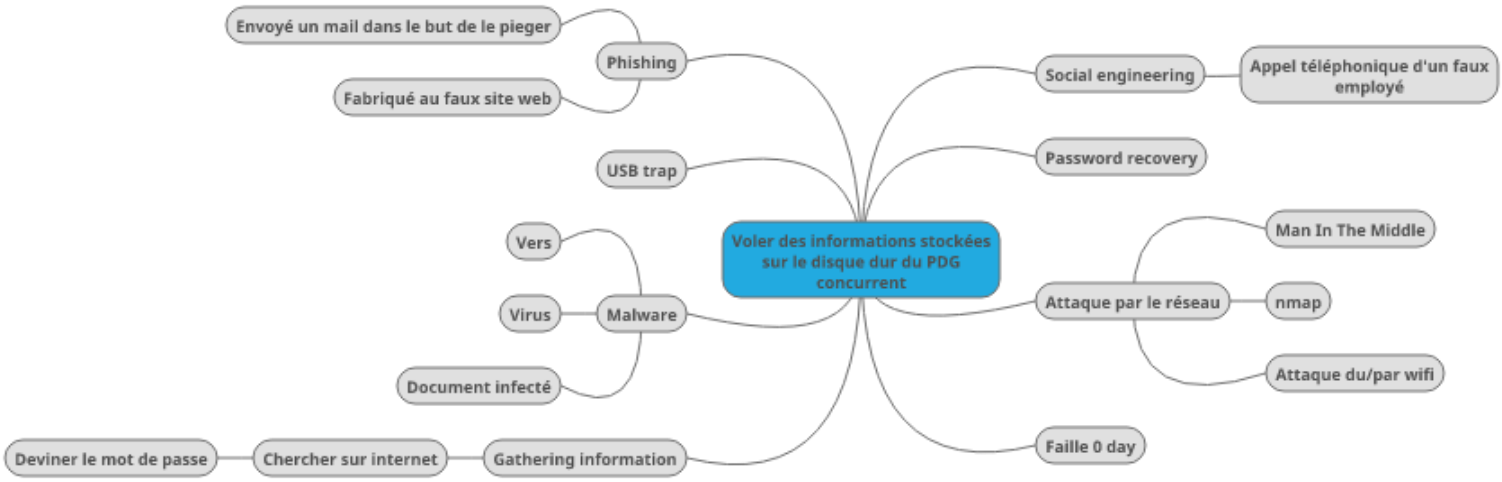
- Both UP
- 1 UP
- Both down
- Recovery

Le schéma suivant montre les transitions entre les différents états des deux serveurs web.



Ex 2

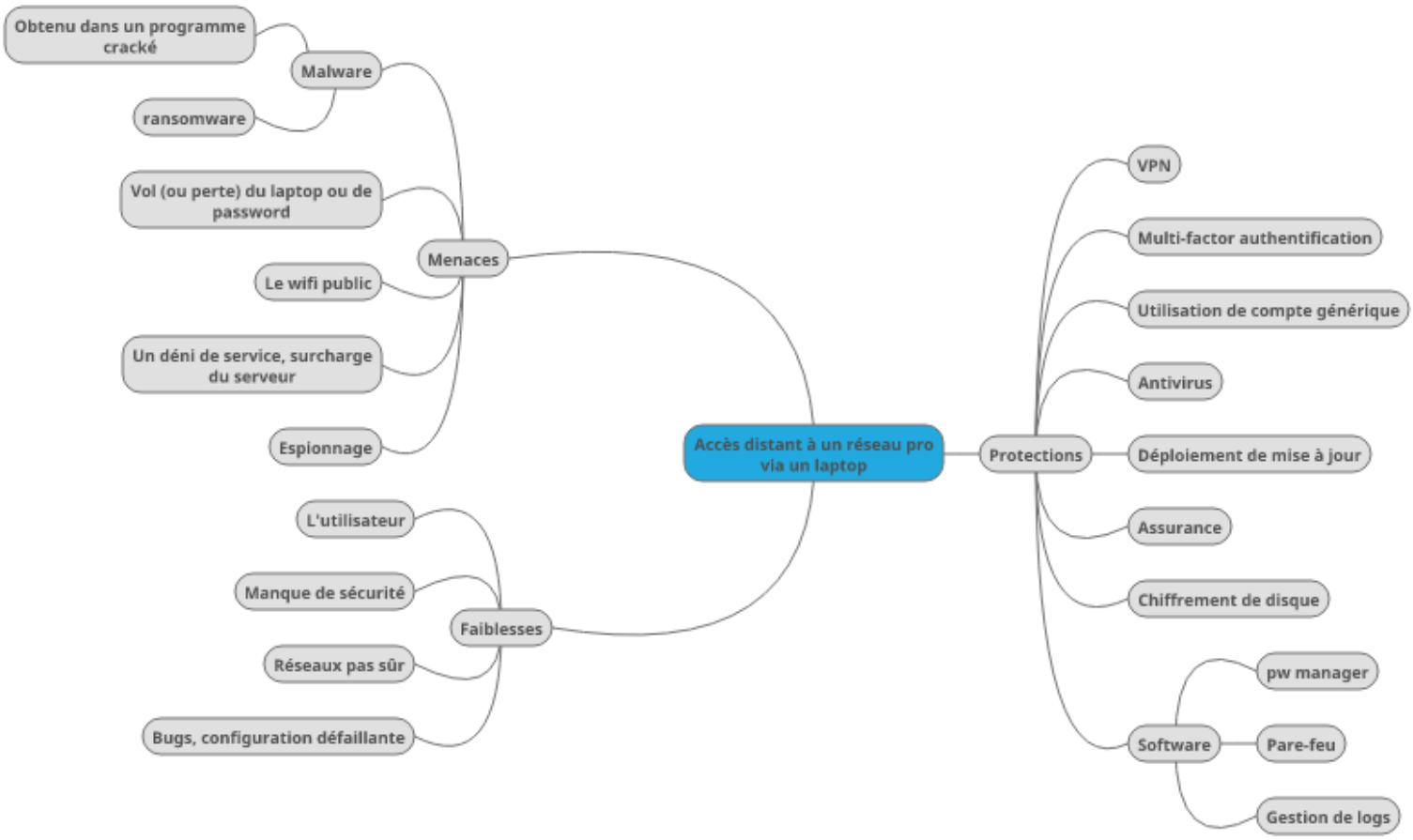
Objectif : Voler des informations stockées sur le disque dur du PDG du concurrent.



Ex 4

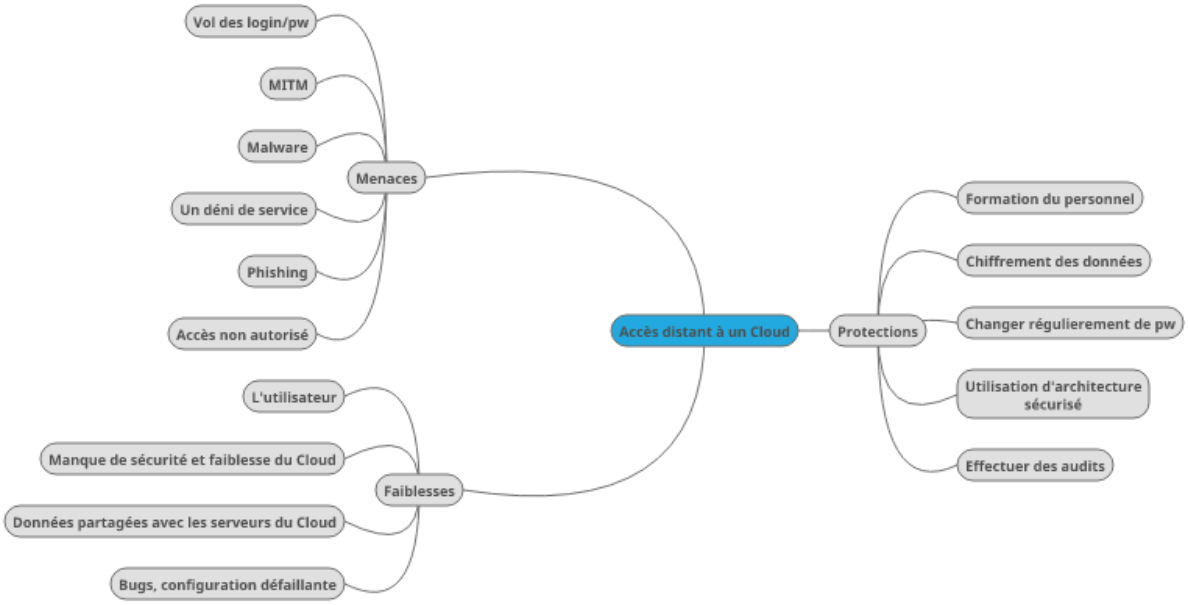
But : mettre en place un accès distant pour des ordinateurs portable appartenant aux employés de l'entreprise.

Périmètre : réseau de l'entreprise en question.



But : utilisation de services de Cloud.

Périmètre : Cloud.



Ex 5

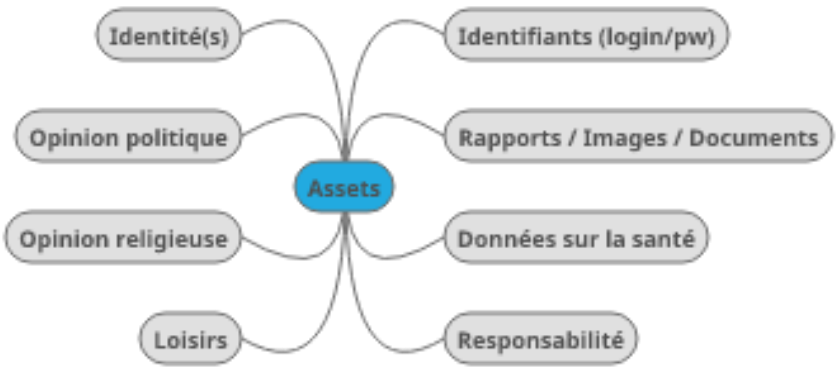
But : Identifier, quantifier et classifier le risque pour les deux scénarios suivants :

- Comme un étudiant en M2 CySec, conduire une analyse de risque sur ses données personnelles en utilisant les ressources informatiques.
- De la même manière, faire une analyse de risque en tant que sysadmin de l'université.

Du point de vue de l'étudiant

Périmètre : téléphone, ordinateur portable, Cloud.

Le mindmap suivant montre les données ayant une valeur.



Liste des menaces et des contre-mesures existantes :

Menaces	Contre-mesures	Vulnérabilités
Vol / perte / casse de l'ordi	Logiciel antivol / Assurance / sauvegardes	Facilité de revente
Malware	Anti-malware / sauvegardes	Utilisateurs / logiciels
Vol / perte des identifiants	Changement de pw / coffre-fort pour pw	keylogger
Phishing	Filtre anti-spam	Utilisateur
Sniffing du réseau	VPN	réseaux

Estimation des problèmes de sécurité :

	Disponibilité	Intégrité	Confidentialité	Performance
User	4	4	4	1

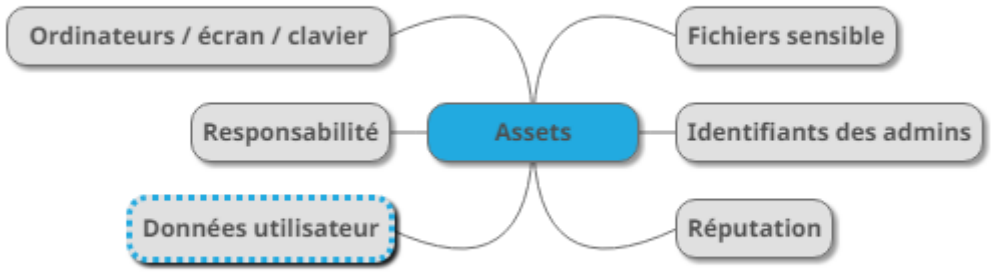
Etapes 5, 6 et 7 :

Menaces	Contre-mesures	Vulnérabilités	Scénarios	Impacts	Probabilités
Vol/perte de l'ordinateur portable	Utiliser un mot de passe de session, logiciel de localisation/wipe, noter l'@ MAC	Facile de le voler et de le revendre	Vol de l'ordi dans le métro, oubli au supermarché	Perte de données et d'argent	3/10
Vol /perte d'identifiants	Changer régulièrement de mot de passe, coffre-fort à mot de passe	Keylogger	Un keylogger envoi les identifiants au pirate	Vol de compte / usurpation d'identité	5/10
Malwares	Antivirus, antimalware, sauvegardes	Beaucoup de malware sur internet, programme cracké	Téléchargement d'un malware dans une version non officiel de Microsoft office	Perte de donnée, violation de la vie privée, dépend du malware	8/10
Mauvaise configuration	Formation, suivre la doc	Utilisateur pas forcement expérimenté	Un pirate infecte un serveur puis les clients à cause de la mauvaise	Attaque massive	7/10

			configuration du serveur		
Phishing	Formation, filtre anti-spam	Utilisateur, adresse URL ambiguë	Mail avec un fausse URL qui demande un login/pw	Usurpation d'identité	6/10
Social engineering	Etre méfiant	L'utilisateur	Un faux employé de la DSI appelle le service comptable demandant des identifiants	Usurpation d'identité, vol de données, détournement de fond	6/10

Du point de vue de l'administrateur

Périmètre : réseau de l'université et accès distant



Liste des menaces et contre-mesures :

Menaces	Contre-mesures	Vulnérabilités
Déni de service	Pare-feu, anti-DDoS	Mise en place rapide
Malwares	Antivirus / antimalwares, mise à jour	Internet, utilisateur
Surcharge	Contrôle de congestion efficace	Infrastructure du réseau
Non disponibilité des données	Load balancing vers un serveur de secours	Hardware
Vol des identifiants admin	Coffre-fort pour mot de passe, authentification multi facteur	Cache, admin

Corruption et perte de données	Sauvegarde (RAID)	Hardware, utilisateur

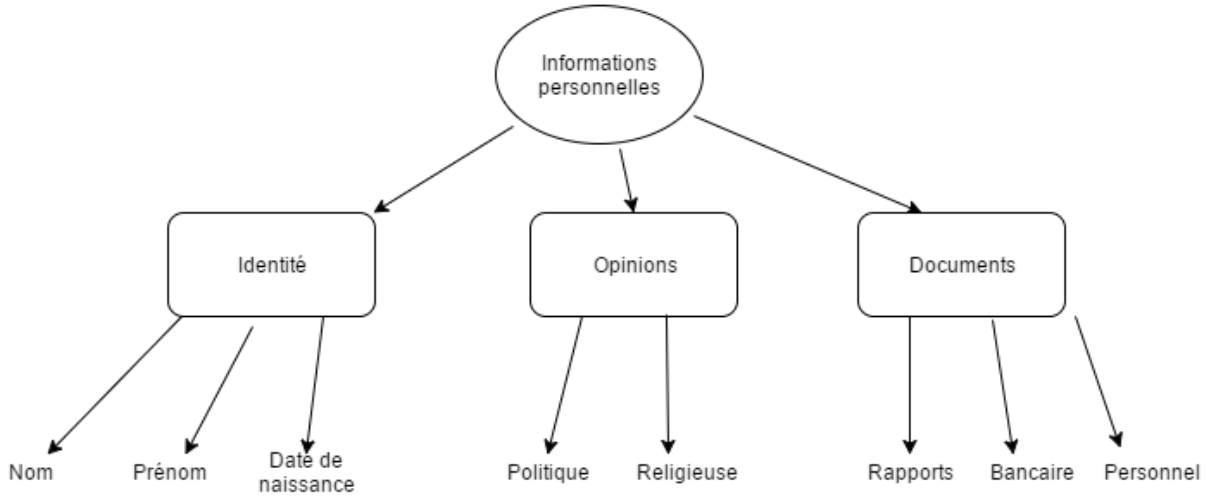
Estimation des problèmes de sécurité :

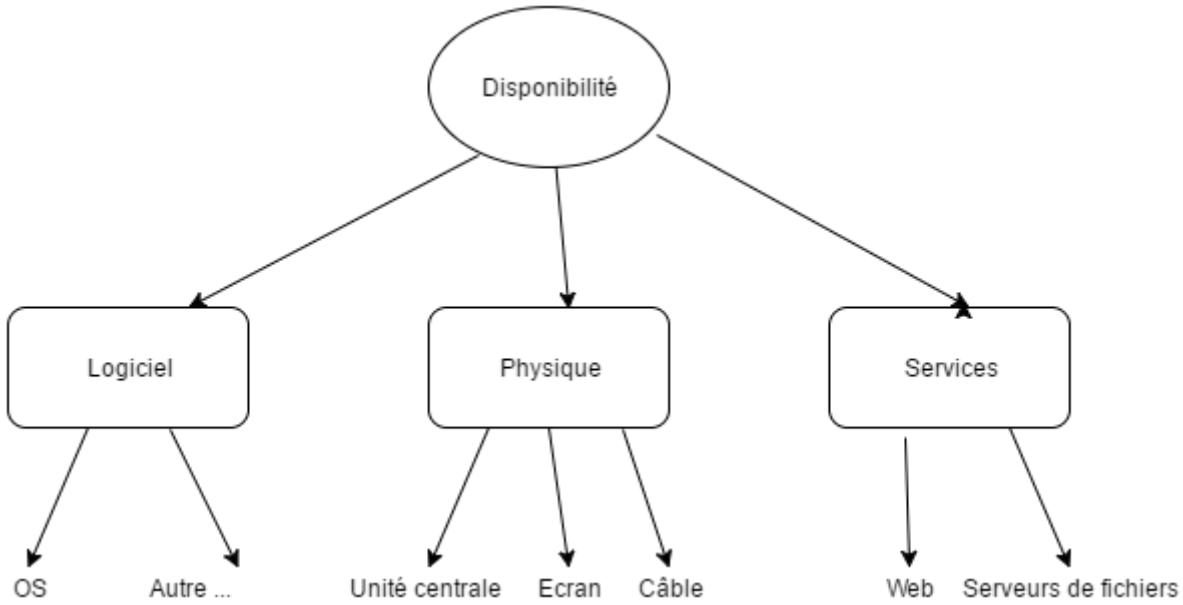
Disponibilité	Intégrité	Confidentialité	Performance
4	1	1	4

Etapes 5, 6 et 7 :

Menaces	Contre-mesures	Vulnérabilités	Scénarios	Impacts	Probabilités
Malware	Antivirus, antimalware, mise à jour	Internet, fichiers corrompus	Clé USB d'utilisateur corrompue	Pertes de données, usurpation d'identité	8/10
Surcharge	Surveillance du réseau, adaptation de l'infrastructure réseau	L'infra réseau	Envoie massive de requêtes par les utilisateurs	Ralentissement des services	4/10
Déni de service	Pare-feu, anti-DDoS	L'infra réseau	Envoie massive de paquet UDP malformé	Cout CPU important rendant indisponible les services	5/10
Indisponibilité des services	Load balancing entre plusieurs serveurs	Hardware	Attaque DDoS extérieur	Ressources non disponible	4/10
Mauvaise configuration	Formation	Admin	L'admin laisse les pw par défauts	Attaque par un pirate	6/10
Perte de données	Sauvegarde (RAID)	Hardware	Disque dur qui ne fonctionne plus	Perte des données, ralentissement des services	3/10
Vol des identifiants admin	Coffre-fort pour mot de passe, authentification multi facteur	Cache, admin	Quelqu'un regarde par-dessus l'épaule de l'admin	Usurpation d'identité	4/10

Exercice 7


Informations personnelles
Identité
Opinions
Documents
Nom
Prénom
Date de naissance
Politique
Religieuse
Rapports
Bancaire
Personnel


Disponibilité
Logiciel
Physique
Services
OS
Autre ...
Unité centrale
Ecran
Câble
Web
Serveurs de fichiers