SAE 1.01 - présentation

BUT RT - Ifs - Clément Brisacier

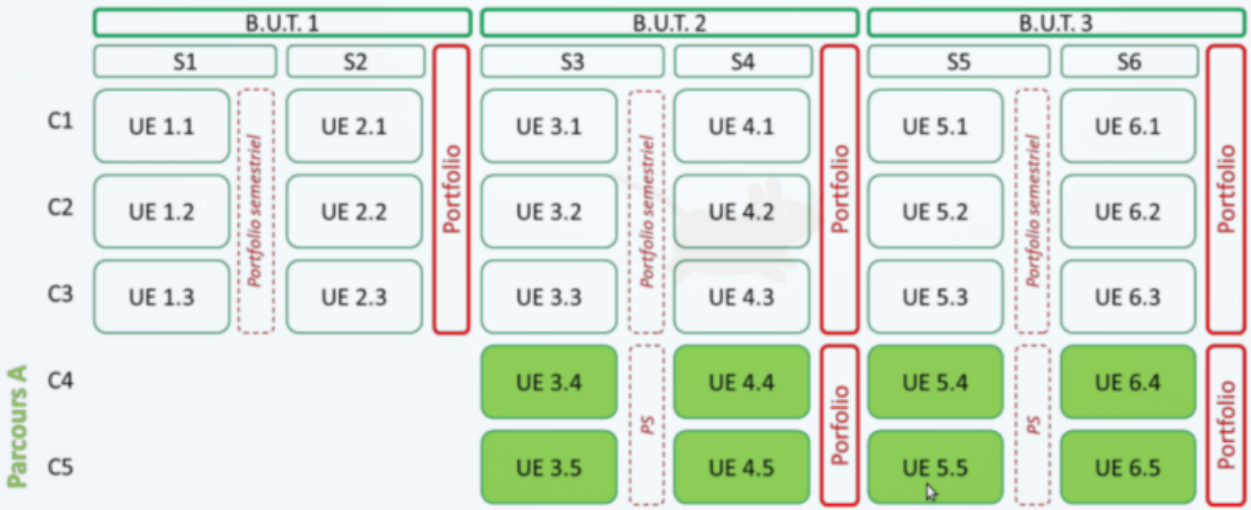
UE et coefficients

– Première année => Tronc commun

– Deuxième et troisième année => Spécialisation

UE et coefficients

- Découpage des années en UE : Unités d'Enseignement (=**compétences**)



- Chaque UE est constituée de deux éléments :
  - un pôle « ressources »,
  - et un pôle « Situation d'Apprentissage et d'Évaluation » (SAÉ).

UE et coefficients

Coefficients du Tronc Commun au S1					
		RT1 - Administrer	RT2 - Connecter	RT3 - Programmer	Total toutes compétences
SAÉ1.01	Se sensibiliser à l'hygiène informatique et à la...	10			
SAÉ1.02	S'initier aux réseaux informatiques	31			
SAÉ1.03	Découvrir un dispositif de transmission		36		
SAÉ1.04	Se présenter sur Internet			8	
SAÉ1.05	Traiter des données			35	
SAÉ1.PORTFOLIO	Portfolio	0	0	0	
R1.01	Initiation aux réseaux informatiques	13	4	4	
R1.02	Principes et architecture des réseaux	12			
R1.03	Réseaux locaux et équipements actifs	7	2	2	
R1.04	Fondamentaux des systèmes électroniques	8	8		
R1.05	Supports de transmission pour les réseaux		6		
R1.06	Architecture des systèmes numériques et...	5		5	
R1.07	Fondamentaux de la programmation			19	
R1.08	Bases des systèmes d'exploitation	6		6	
R1.09	Introduction aux technologies Web			4	
R1.10	Anglais technique 1	5	5	5	
R1.11	Expression-Culture-Communication...	4	5	5	
R1.12	Projet Personnel et Professionnel	2	2	2	
R1.13	Mathématiques du signal	5	9		
R1.14	Mathématiques des transmissions	5	9		
R1.15	Gestion de projet 1 : Maîtriser les bases de...		3	3	
	Total sur les SAEs	**41**	**36**	**43**	120
	Total sur les ressources	**72**	**53**	**55**	180
	Total sur les SAEs et les ressources	**113**	**89**	**98**	300

SAE1.01

SAE : Situation d'Apprentissage et d'Evaluation

- Apprentissage, production, évaluation (projet !)
- Approche par compétences
- Souvent en groupe, parfois en autonomie
- Utilisation des "Ressources" acquises : R101, R108, etc.
- S1 : 6 SAE

SAE1.01 : descriptif

"Se sensibiliser à l'hygiène informatique et à la cybersécurité"

Coefficients	RT1 : coeff. **10**

Objectifs et problématique professionnelle

Le professionnel R&T est l'un des premiers interlocuteurs des nouveaux collaborateurs arrivant au sein d'une entreprise, ces derniers étant confrontés aux risques potentiels de leur environnement numérique. Il doit les sensibiliser aux bonnes pratiques de l'hygiène informatique et leur faire adopter les bons réflexes afin qu'ils deviennent des collaborateurs conscients, avertis et responsables de l'environnement numérique. Il doit en outre faire connaître et accepter la charte informatique imposée par la Direction des Systèmes d'Information (DSI).

Description générique

Description

Le professionnel R&T est confronté aux risques qu'il peut encourir s'il ne considère pas avec attention l'usage de son environnement numérique. Par une approche éducative et technologique, il doit prendre connaissance des menaces numériques communes (cybersécurité) et savoir les actions à mettre en place pour y remédier. Il est capable de présenter à ses collaborateurs de façon claire, concise et vulgarisée les menaces et les attaques communément employées sur les réseaux numériques.

Type de livrables ou de productions

Les étudiants peuvent produire :

- un rapport d'analyse des risques numériques
- une présentation diaporama
- une courte vidéo de sensibilisation (par ex : «en 180 secondes») destinée à vulgariser les premiers pas en cybersécurité.

L'étudiant s'approprie son portfolio. Des temps sont prévus pour qu'il y synthétise sa production technique et son analyse argumentée.

Mots-clés

Sécurité numérique, Utilisation d'Internet, Menaces communes, Remédiations.

SAE1.01 : contenu

L'idée est d'obtenir une bonne hygiène de l'utilisation des services numériques et d'être capable de former des utilisateurs non spécialistes à ces bonnes pratiques.

3 travaux principaux :

- auto-formation individuelle au MOOC de l'ANSSI
- travail de préparation en groupe autour de thématiques "cyber" et présentation du travail sous forme d'oral de groupe
- TP de découverte style "Capture the Flag"
- ... plus un QCM en fin de SAE

Déroulé et notation

- 1h de CM
- 12h de projet en autonomie
- 2h de TP (23/10) : CTF
- 1h de TP (24/10) : présentation de l'oral noté de groupe
- 1h de QCM (24/10)

SAE1.01

Travail en groupe et/ou en autonomie :

- heures de projet dédiées (12h)
- autonomie = pas d'enseignant !
- à vous de vous responsabiliser sur le matériel et le travail
- à disposition : machines locales, VM sur le Proxmox
- en cas de soucis : mail à l'enseignant

ANSSI

1. **Défendre...**

   - ...les systèmes d'information critiques de la Nation en concevant et opérant le déploiement de capacités de détection des cyberattaques ;
   - ...les victimes de cyberattaques d'ampleur ;
   - ...la Nation en structurant au niveau national l'assistance aux victimes de cyberattaques.

2. **Connaître...**

   - ...l'état de l'art en sécurité des technologies et des systèmes d'information et en être des experts ;
   - ...les menaces et les risques dans le cyberespace et développer des méthodes et des outils pour y faire face ;
   - ...les tendances du monde de la cybersécurité, en France, en Europe et à l'international, pour s'y inscrire pleinement en défendant une vision singulière de la sécurité et de la stabilité du cyberespace.

3. **Partager...**

   - ... des recommandations de cybersécurité, des solutions et des outils aux acteurs de la cybersécurité et de la transformation numérique pour démultiplier l'action de l'agence et renforcer la cybersécurité collective ;
   - ...sur la réponse à la menace au sein des réseaux de coopération techniques, opérationnels et stratégiques français, européens et internationaux ;
   - ... l'expertise de l'agence dans le domaine de la cybersécurité pour former les agents de l'État et des opérateurs régulés à la cybersécurité ;
   - ...largement les connaissances en matière de cybersécurité et encourager le développement de la filière et des formations en cybersécurité ;
   - ..., en lien avec ses partenaires, pour informer et sensibiliser les citoyens aux risques cyber.

4. **Accompagner...**

   - ...le développement d'une doctrine française de cybersécurité et la conception des dispositifs normatifs et réglementaires aux niveaux national et européen ;
   - ...le Gouvernement dans le déploiement d'une politique publique en matière de cybersécurité ;
   - ...les plus hautes autorités dans leur appréhension du fait cyber ;
   - ...les opérateurs régulés dans l'application des mesures de sécurisation de leurs systèmes d'information et leurs réponses aux incidents ;
   - ...le développement d'un écosystème de prestataires de produits et de services de confiance dans le domaine de la cybersécurité.

MOOC

MOOC : Massive Open Online Course. Différentes ressources autour de l'hygiène numérique : vidéos, présentations, quizz, etc.

MODULE 1
Panorama de la sécurité des systèmes d'information (SSI)

- **Unité 1** : un monde numérique hyperconnecté
- **Unité 2** : un monde à hauts risques
- **Unité 3** : les acteurs de la cybersécurité
- **Unité 4**: protéger le cyberespace
- **Unité 5** : les règles d'or de la sécurité

MODULE 2
Le b.a.-ba de l'authentification

- **Unité 1** : les principes de l'authentification
- **Unité 2** : attaques sur les mots de passe
- **Unité 3** : sécuriser son mot de passe
- **Unité 4** : gérer ses mots de passe
- **Unité 5** : pour aller plus loin : notions de cryptographie

MODULE 3
Sécurité sur Internet : les bons réflexes

- **Unité 1** : Internet, de quoi s'agit-il ?
- **Unité 2** : les fichiers en provenance d'Internet
- **Unité 3** : la navigation web
- **Unité 4** : la messagerie électronique
- **Unité 5** : pour aller plus loin : l'envers du décor d'une connexion web

MODULE 4
La sécurité : partout, tout le temps

- **Unité 1** : sécurité du poste de travail
- **Unité 2** : le réseau domestique
- **Unité 3** : les objets connectés dans la maison
- **Unité 4** : mobilité
- **Unité 5** : pour aller plus loin : la séparation des usages.

Rendez-vous sur www.secnumacademie.gouv.fr

Attendus

- Objectifs :
  - Préparer la séance de "Mise en situation professionnelle" (TP) par un travail de recherche et d'expérimentation
  - Préparer un document technique résumant le travail réalisé
  - Mutualiser à l'oral au sein du groupe TP le travail réalisé
- Créer 3 groupes de 3 à 5 personnes par groupe de TP. Taille du groupe uniforme autant que possible.
- Répartir les lots A, B et C
- Produire une notice (document collaboratif en ligne) par groupe pour chaque lot
- Présenter un résumé de cette notice sous la forme de quelques diapositives lors la séance d'oral qui sera encadrée par un enseignant

Lot A : Mots de passe utilisateurs

Travail de recherche et d'expérimentation :

- Bonnes pratiques : Complexité des MDP, force, renouvellement, moyen mnémotechnique etc.
- Force brute et dictionnaire : Décrire concrètement à partir d'un logiciel disponible sur Debian comment réaliser une attaque par force brute, à partir de données personnelles et d'un dictionnaire...
- Gestion des mots de passe :
  - Décrire les principales fonctionnalités offerte par un gestionnaire de mot de passe
  - Décrire les logiciels disponibles sur une distribution Debian pour gérer ses mots de passes.
  - Mettre en œuvre un gestionnaire de mot de passe

Lot B : Accès SSH

Travail de recherche et d'expérimentation :
Décrire sur un logiciel serveur et client SSH comment :

- Renforcer la sécurité de la connexion : Port, algorithmes, blocage si n tentatives, protection des clés, etc.
- Remplacer le login/password par une clé publique/privée : Explique les mécanismes, insister sur les algorithmes préconisés par l'ANSSI et la taille des clés

Lot C : Découvertes de machines (mais pas que)

Travail de recherche et d'expérimentation :
Décrire concrètement à partir de logiciels disponibles sur une distribution Debian comment réaliser les actions ci-dessous:

- Découvrir les machines du réseau
- Découvrir les OS des machines du réseau (Fingerprint)
- Découvrir les services disponibles
- écouvrir les logiciels utilisés, et si possible leur version

Conclusion

- MOOC à préparer
- groupes à constituer et choix des lots
- travail de recherche et préparation d'un oral
- des questions ?