Quatrième période du 11-03-2024
au 12-04-2024 (5 semaines)

Rapport des enseignements à l'IUT

Alexis Déhu
adehu@univ-pau.fr

Enseignant référent :

M. Angel Abénia
abenia@univ-pau.fr

du 11 Mars, au 12 Avril 2024

Alexis Déhu

Rapport des enseignements à l'IUT

Le présent document est le compte rendu de mes enseignements reçus à l'IUT de Mont-de-Marsan pour la quatrième période d'apprentissage allant du 11-03-2024 au 12-04-2024 en deuxième année de BUT Réseaux & Télécommunications.

du 11 Mars, au 12 Avril 2024

Cet apprentissage en alternance a été réalisé dans le cadre de l'obtention d'un BUT en Réseaux & Télécommunications à l'Université de Pau et des Pays de l'Adour, IUT de Mont-de-Marsan. La période d'alternance d'une durée de 2 ans s'est établie du 1er Septembre 2023 au 31 Août 2025 dans les locaux de ADITU, Technopole Izarbel Côte Basque, 64210 Bidart.

Aucune intelligence artificielle n'a été utilisée pour la rédaction ou l'aide à la production de ce document. Aucune information présente n'a été récupérée brute de forme depuis quelconque source, publique ou non. Ce document est le fruit d'un travail personnel et que je n'ai ni contrefait, ni falsifié, ni copié tout ou partie de l'œuvre d'autrui afin de la faire passer pour mienne.

Un immense merci à mon enseignant référent à l'IUT.

M. Angel Abénia - Enseignant chercheur

du 11 Mars, au 12 Avril 2024

Résumé des enseignements

Cette deuxième période la plus longue d'enseignements à l'IUT (5 semaines) nous a permis d'aborder un vaste champ de compétences extrêmement utiles et intéressantes selon moi.

Nous avons couvert trois modules de notre parcours cybersécurité orienté vers la sécurisation du service DNS avec DNSsec, de la compréhension des attaques utilisées sur des protocoles répandus dans les réseaux locaux d'entreprises et de la compréhension des technologies et pratiques de chiffrement de nos données.
Nous avons aussi aussi à manipuler et intégrer des pare-feux physiques dans un réseau local d'entreprise selon leur besoins.

Aspect télécommunications, nous avons abordés les réseaux cellulaires 2G, 3G, 4G et d'autres en profondeur, en parallèle avec l'étude physique et mathématique de moyens transmissions modernes d'émission-réception.

Un module intéressant était aussi consacré à l'automatisation de nos tâches d'administrations des systèmes et des réseaux. En complément de l'apprentissage d'un anglais professionnalisé et d'un travail sur notre communication.

Secteurs d'enseignements: sécurisation; protocoles; ARP; ICMP; DNS; chiffrement; cryptographie; clés; chiffrement symétrique; chiffrement asymétrique; intégrité des données; confidentialité; authentification; authenticité; signature; certificat; fonctions mathématiques et algorithmiques; OFDM; COFDM; MIMO; CDMA; TDMA; FHSS; féseaux cellulaire; filtres numériques; filtres analogiques

Table des matières

1

R4Cyber.09 Sécurité des Réseaux LAN (16h30)

Enseignant
M. Laurent Gallon

Ce module portait sur la sécurisation des réseaux locaux d'entreprise. Dans celui-ci, nous avons revu le fonctionnement de protocoles réseaux utilisés dans les réseaux locaux d'entreprise, pour ensuite en voir une application utilisée pour des attaques courantes les utilisant.

Pour se prémunir de ces attaques et mieux les comprendre, nous les avons expérimentées dans des environnements contrôlés, puis nous avons mis en place des mécanismes de protection pour s'en prémunir.

1.1 Forger des paquets volontairement malicieux sur un réseau

Pour simuler les attaques, nous avons appris à initier un comportement anormal sur un réseau en modifiant les informations que l'on envoie sur celui-ci.

Notre intention dans une attaque est de générer un comportement anormal sur une machine ciblée. Pour ce faire, nous devions forger des demandes malicieuses pour provoquer une réaction attendue chez elle.

Nous avons donc appris à utiliser l'outil `Scapy` pour générer tout type de trafic réseau, en modifiant à souhait la composition de nos demandes. Nous pouvions notamment à l'issue usurper

l'identité d'un hôte sur le réseau pour que celui-ci reçoive des communications que nous avions initiées à sa place.

1.2 Prise en main des attaques courantes

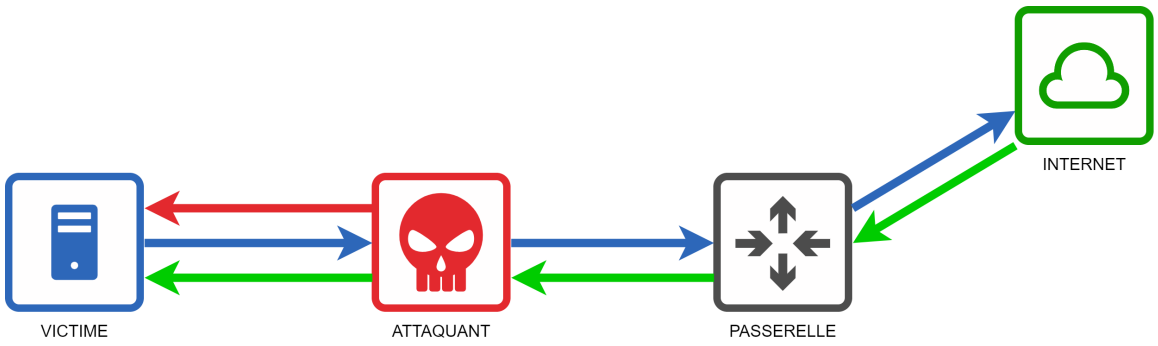
Suite à cet apprentissage, nous avons pu commencer notre étude des attaques étudiées théoriquement. Nous en avons notamment montées deux : l'attaque de l'homme du milieu par empoisonnement de la table ARP, et l'attaque du déni de service par rebond. Je vais en présenter une ici.

1.2.1 Attaque de l'homme du milieu par empoisonnement ARP

Pour la première, il nous fallait revoir le fonctionnement du protocole ARP. Celui-ci est indispensable pour utiliser le protocole IPv4, servant à trouver qui possède une adresse IP dans un réseau local.

Notre objectif, côté attaquant, fut de dire dans un réseau local à toutes les machines que nous étions maintenant leur passerelle, ou leur "box". Nous disions à haute voix notre nouvel emplacement pour usurper identité de la vraie passerelle, afin que les machines pensent que si elles veulent accéder à Internet, qu'elles le fassent par nous.

Nous avions par la suite qu'à renvoyer les demandes de connexion vers la vrai passerelle, et renvoyer les réponses aux victimes. Nous pouvions donc voir les connexions que les machines effectuées sur Internet, et si non protégées : voir leur contenu.



1.1: Illustration de l'attaque par l'homme du milieu par empoisonnement de table ARP. L'attaquant informe qu'il est le nouvel emplacement de la passerelle du réseau pour intercepter les requêtes et les réponses attendues pour la victime.

2

R4Cyber.10 Cryptographie (10h30)

Enseignant
M. Laurent Gallon

Ce module nous a plongé dans la compréhension des fondamentaux de la cryptographie, à l'intérieur du chiffrement de nos données. Nous y avons abordé les principes d'authenticité, de confidentialité et d'intégrité des informations transférées lors d'un échange.

La cryptologie a été abordée via une approche scientifique et mathématiques théoriques dans un premier temps, puis par une approche pratique avec une application dans un système de messagerie et de connexion à des machines distantes sécurisée.

2.1 Enseignements théoriques

Lors des travaux pratiques et des cours magistraux, nous avons vu les schémas de fonctionnement des algorithmes courants de cryptographie, des fonctions de hachage et de la chaîne PKI.

Nous avons étudié les protocoles RSA et Diffie-Hellman pour nous intéresser à la cryptographie. Le premier de la famille des clés symétriques et le deuxième des asymétriques, leur objectif commun est de former un couple de clés (distrinctes pour l'asymétrique, identiques pour la symétrique) que seuls les communiquant connaîtront et utiliseront pour s'échanger des informations.

Problème de la clé symétrique : on ne peut pas distinguer l'une personne de l'autre utilisant

la clé. Ainsi, la paire de clés asymétriques permet une authentification de l'expéditeur du message, utilisant sa clé unique privée pour chiffre son message que le ou les réceptionneurs pourront déchiffrer s'ils ont en leur possession une clé dite "publique" que tout le monde pourra utiliser pour ouvrir le message chiffré.

Le système de chiffrement asymétrique est notamment utilisant lors de vos navigations WEB pour être certain de l'identité de `google.com` par exemple : tout le monde est en possession de la clé publique sur leur navigateur mais uniquement `google`, qui lui seul possède sa clé privée, pourra initier un échange chiffré (et non un autre site usurpateur).

2.1.1 Application dans le monde réel

Nous avons appliqué les concepts dans le cadre de chiffrement de courriels entre deux adresses. En effet, toujours en suivant le principe des clés asymétriques : nous avons vérifié l'authenticité de l'expéditeur, l'authenticité du message mais aussi son intégrité en vérifiant son empreinte.

La vérification de l'empreinte permet de vérifier si le message a été modifié en cours de route. Cependant, celui-ci ne doit pas être modifié lui aussi... C'est pour cela que lui aussi est chiffré avec le message pour que le destinataire en déchiffrant le message puisse le comparer à son empreinte et être certain de son intégrité.

3

R4Cyber.11 Sécurisation des services réseaux (16h30)

Enseignant
M. Jean-Jacques Bascou

Nous avons étudié pour le module R4Cyber.11 des principes de sécurisation d'un protocole constamment utilisé mais protégé que tardivement : le protocole DNS.

Le protocole DNS sert à effectuer des résolutions de noms sur Internet. Pour donner un exemple, vous retenez le nom symbolique `youtube.com` pour accéder aux serveur de YouTube; et non pas les adresses IP des serveurs sur Internet. Les serveurs DNS servent à faire correspondre des noms symboliques à des adresses IP tangibles par vos machines.

Les noms symboliques fonctionnent par arborescence. Pour 'www.univ-pau.fr', en premier sera demandé le serveur DNS gérant `.fr` pour lui demander l'emplacement de `univ-pau` (l'adresse IP du serveur DNS gérant cette zone de sites), qui lui saura nous dire pour quelle adresse IP il possède un enregistrement pour `www`.

Ainsi, si les serveurs dirigeants vers les `.fr`, les `.com` etc. tomberaient en panne : plus personne ne saurait savoir où sont les sites sur Internet (à moins de déjà connaître leurs adresses). Pour ce faire, sont utilisés et connus 13 serveurs DNS dit racines, gérés par les plus grandes sociétés pour que la résolution des noms puissent toujours opérer sur Internet. Nous faisons confiance à la sécurité de ces 13 serveurs, leur disponibilité et leur véracité : mais quand est-il si l'on doit le faire pour nous ?

Ainsi, nous avons pu commencer à gérer notre zone DNS (par exemple `adehu.univ-pau.fr`) et la sécuriser avec DNSSEC; qui est une suite de bonnes pratiques pour sécuriser son installation DNS.

Ainsi, nous avons vu comment authentifier nos serveurs DNS entre eux pour éviter qu'une personne mal intentionnée puisse se faire passer pour un serveur DNS voulant redistribuer nos informations. Signer nos zones gérées en utilisant une information donnée par le serveur DNS supérieur (dans notre exemple du `adehu.univ-pau.fr`, j'utilise une information de `univ-pau` pour lui dire que je gère bien (et moi seul) `adehu`..

4

R4.01 Infrastructures de sécurité (7h30)

Enseignant
M. Laurent Gallon

Présent dans le tronc commun mais faisant appel aux notions de notre parcours Cybersécurité, le module Infrastructures de sécurité nous a plongé dans le fonctionnement des chiffrements de nos données et à la découverte des équipements et des principes de sécurité permettant la sécurisation de nos transmissions et des infrastrctures.

Ainsi, nous avons abordés l'ensemble des informations permettant la compréhension des mécanismes de filtrage et de contrôle des accès d'un réseau, les bases de la cryptographie, ainsi que les services, applications et infrastructures pour la sécurité.

4.1 Enseignement et manipulation de pare-feux

Nous avons pu voir en détail les métholodologies d'approche des règles d'un pare-feux, à mémoire d'états ou non. Un pare-feu se définit comme un équipement régissant les flux d'accès dans un réseau : telle personne a le droit d'accéder à cette ressource, celle-ci ne doit pas y accéder ou n'a pas besoin de cet accès...

Un pare-feu matériel n'est pas à confondre avec un pare-feu logiciel comme présent sur vos ordinateurs; ceux-ci régissent les activités des programmes installés sur vos machines, un équipement pare-feu régit l'activité d'un réseau pour gérer les flux et les accès.

Dans cette vision, nous avons élaboré des stratégies de sécurisation d'entreprises à moyenne

et grande échelle. Nous y avons vu la réflexion derrière la confection d'un tableau de gestion d'accès, et son implémentation sur une machine pare-feu GNU/Linux.

Plusieurs notions avancées ont été couvert comme les DMZ *zones démilitarisées* pour laisser une activité extérieure accéder à certaines ressources en dehors du réseau d'entreprise (dans le cas d'un hébergement dans les locaux d'un site WEB, d'une application métier...). Nous avons aussi couvert le NAT *translatation d'adresses*, les ACL *règles d'accès* et les firewall-proxy pour restreindre les applications dans leur fonctionnement sur le réseau.

Nous avons ainsi mis en place lors de travaux pratiques une connexion multi-site via un réseau d'opérateur avec un accès distant sécurisé, des services réseaux avancées; tout cela en mettant en place une politique de sécurisation et de contrôles d'accès via des firewall-proxy.

5

R4.02 Transmissions avancées (24h)

Enseignant
M. Christophe Baillot

Module d'enseignement portant sur la physique des télécommunications, nous y avons abordé les prémices des notions relatives à la transmission sur antennes pour de la radiophonie, de la téléphonie et des données (Wi-Fi...).

Pour cela, nous avons revu les systèmes d'émission et réception sur des systèmes modernes par les filtres numériques; et plus particulièrement en abordant dans les domaines mathématique et physique le fonctionnement de la modulation IQ.

Par la suite, nous avons commencé à voir les problématiques liées à l'utilisation de l'espace comme support de transmission. Nous y avons premièrement abordé la problématique des chemins multiples d'une onde dans un milieu urbain, ainsi que les technologies qui ont permis de s'en prémunir.

La suite de ce module fut celui R4.03, où nous continuions notre avancée prise par l'apprentissage sur ce module.

5.1 Les émetteurs-récepteurs de systèmes modernes (filtres numériques)

Pour revoir les émissions et les réceptions théoriquement, nous avons abordé de manière poussée la modulation IQ. En effet, la modulation permet à une suite d'information d'être modifiée pour

mieux circuler sur son support (ici, l'air).

La modulation IQ elle se sert de la phase d'un signal pour définir ses états significatifs (0, 1; ou 00, 01, 11...) que l'on devra discerner à la réception pour interpréter le signal, et retrouver les informations.

Dans cette optique, nous avons d'abord étudié physiquement le schéma comportemental de l'émission sur modulateur IQ, en représentant dans l'espace des fréquences et du temps le signal à différents endroit du dispositif.

Nous avons par la suite caractérisé mathématiquement la raison du comportement du signal à ces emplacements, suite de multiplication par des sinusoïdes à l'envoi et la réception.

En conséquent, nous avons étudié en profondeur le fonctionnement et la mathématique d'un système de transmission en télécoms, la modulation IQ. Extrêmement enrichissant et contingent à la compréhension des composant d'un système (filtres, amplificateurs, mélangeurs, oscillateurs locaux...).

5.2 Gestion des problématique des télécoms dans les airs

Chaque support de transmission a ses avantages et ses inconvénients, l'air ne faisant exception. Nous avons commencé à aborder une des problématiques majeures que procure l'air à son utilisation : une onde se propage librement dans l'air, si relief urbain celle-ci peut rebondir sur les bâtiments et revenir à la réception plusieurs fois dû au temps des différents trajets qu'elle aura emprunté.

Le problème des trajets multiples a été contré dès la 2G avec les sauts de fréquences (FHSS, 1 message une fréquence et on tourne), avec de l'étalement de spectre CDMA pour la 3G et l'OFDM avec son attente pour la 4G.

Nous avons étudié ces trois technologies, leurs fonctionnement évolutions et avantages au fil du temps, sur le plans physiques notamment. Nous avons aussi entrevu la CDMA utilisé sur du Wi-Fi, Wimax et 5G.

6

R4.03 Physique des télécoms (27h)

Enseignant
M. Christophe Baillot

Pour ce deuxième module exclusif à la physique des télécoms, nous avons abordés des notions avancées en électronique touchant globalement aux réseaux cellulaires dans les télécoms, faisant sens à notre module R4.04 et R4.02.

Nous y avons vu les émetteurs et récepteurs superhétérodynes et 0 IF, de la modulation multiporteuse OFDM

6.1 Les systèmes de transmission étudiés

Nous avons étudié les systèmes de transmission superhétérodynes, en soit des systèmes de transmission modulant deux fois le signal sur une fréquence porteuse et sur une fréquence intermédiaire, cette dernière pour le transport.

Leur intérêt est de pouvoir recentrer le signal sur une fréquence particulière tout en conservant la modulation permise par la fréquence porteuse. À la réception, remultiplier le signal reçu par la même fréquence intermédiaire permettra avec un filtre de récupérer le signal transporté avec transposition.

Le récepteur 0 IF, pour aucune fréquence intermédiaire (ou image), permet de récupérer le signal modulé en bande de base en échantillonnant de telle sorte que le repliement de spectre permette que le signal reçu s'amplifie en `0 Hz`.

Ce dernier est utilisant à très hautes fréquences, les systèmes actuels ne pouvant échantillonner des valeurs arrivant aussi rapidement (à hautes fréquences).

Ainsi, nous avons vu successivement plusieurs technologies, chacune répondant petit à petit à des problématiques grace aux avancées faites

6.1.1 Compréhension des principes liés au MIMO

Nous avons finalement abordé les technologies MIMO et MISO, utilisant des émetteurs à plusieurs antennes, et/ou non des récepteurs à plusieurs antennes aussi.

Leur utilisation permette de mieux recevoir le signal, et d'en diminuer le rapport que l'on en voit avec le bruit. Ou d'envoyer une information d'antenne à antenne quand le nombre est réciproque des deux côtés (en décorélant les flux, envoyer X fois plus d'informations où X le nombre d'antennes).

7

R4.04 Réseaux cellulaires (27h)

Enseignant
M. Yannick Lespine

Grand module dans les télécommunications, celui-ci nous a énormément appris sur les réseaux cellulaires notamment pour la téléphonie mobile. Reprenant des enseignements sur les antennes et la physique permettant le transport d'informations, le module R4.04 nous a plongé dans la compréhension des réseaux mobiles 2G, 3G et 4G; avec des parties applicables au Wi-Fi.

Est entendu réseau cellulaire un réseau couvrant une surface, découpé en petites zones alors dites cellules pour couvrir l'ensemble de la surface.

Ce principe est utilisé dans la téléphonie mobile (3G, 4G...). Ainsi, vous avez des antennes partout en France permettant de couvrir globalement le territoire. Les antennes couvrent une cellule.

Appliqué à ceci, nous avons vu l'intérêt des pylônes pour les opérateurs et pourquoi sont-ils si haut. Nous avons aussi vu les ondes et fréquences délimitant les normes (GSM, 3G, 4G...), les technologies que celles-ci utilisent et ce très en profondeur.

Ainsi, nous avons vu en détails toutes les procédures de communication entre un appareil mobile, un pylône et le réseau, pour transférer de la données ou de la voix et les problèmes que cela engendre sur de grandes distances (chemins multiples). Nous avons notamment étudié comment un téléphone se raccorde à une antenne, comment le faire sonner, que ce passe-t-il lorsqu'il est en déplacement (voiture ou autre) et que l'on est en communication.

En travaux pratique, à l'aide d'analyseur de spectres : nous avons étudiés les signaux reçus des antennes aux alentours et comparé nos résultats avec nos connaissances. Nous avons aussi étudié la couverture réseau entre les villes de Mont-de-Marsan et Dax, les intérêts des opérateurs selon tels pylônes, couvertures...

8

R4.05 Automatisation des tâches d'administration (7h30)

Enseignant
M. Philippe Arnould

Initié cette période mais finalisé celle suivante, ce module abordait l'automatisation de nos tâches d'administration systèmes et réseaux. Ainsi, nous avons montés des infrastructures sur lesquels nous avons utilisé des API, des scripts ou du code pour effectuer en une manipulations des actions qui auraient été répétitives et longues si faites manuellement sur chaque équipement.

En conséquent, nous pouvions déployer nos actions sur plusieurs machines simultanément, sans avoir à manuellement répliquer chaque configuration, préparer une sauvegarde, sauvegarder la configuration manuellement à chaque passage...

8.1 Prise en main d'outils d'automatisation

Plusieurs outils nous ont permis d'automatiser nos tâches : des API et des intégrations. Nous avons majoritairement pris en main Ansible et paramiko pour nos manipulations.

8.2 Principde de fonctionnement des API

Les API sont des interface exposées à l'extérieur d'une machine, que l'on peut appeler pour lui demander d'effectuer une ou plusieurs manipulations en interne. Ainsi, en donnant une suite d'instruction à faire à une API, celle-ci pourra l'appliquer à l'équipement et nous en renvoyer

le résultat.

L'intérêt des API est de pouvoir être appelées par différent supports (différents langages de programmations, solutions, programmes, humains ou non) et de permettre une réplication de l'instruction à d'autres équipements (un programme va contacter 100 équipements où il faut changer une information).

8.2.1 Intégrations que nous en avons fait

Nous avons aussi manipuler des intégrations de protocoles que nous utilisions déjà. Nous avions l'habitude d'ouvrir une session de connexion à distance SSH à nos machines pour leur renseigner des actions à effectuer pour changer leur état. Aujourd'hui, nous pouvons générer du code informatique qui va lui-même aller le renseigner à différentes machines et nous renvoyer le résultat.

Ceci permet de ne pas avoir à passer 50, 100 machines manuellement pour répéter le même processus. Des outils comme `paramiko` ou `netmiko` automatise nos tâches sur SSH par exemple. Sans oublié les indispensables `Ansible` (beaucoup utilisé), `Puppet` ou `Cheff` pour la gestion d'un parc, qui peuvent faire appel à des applications comme paramiko et netmiko.

Des notions plus avancées et standardisées peuvent être amenées à être utilisés mais non abordés à l'IUT, `netconf` (ssh) et `restconf` (http). Ceux-ci sont des protocoles dédiés à la standardisation d'accès aux informations de tout équipement confondu, de pouvoir changer leur état sans changer les instructions qu'on donne pour chaque constructeur... Tout cela dans le modèle d'application `YANG`, qui donne la structure à utiliser pour effectuer des appels à consultation ou modifications. Souvent couplé au modèle `Agile` qui définit les bonnes pratiques à avoir lors d'appels à ces protocoles (sauvegarde, tests de vérification après application, rédaction d'un rapport...).

9

R4.06 Anglais professionnel (15h)

Enseignant
Jeff

Reprenant les pas du module R3.11, Jeff a repris ses exercices de grammaires et les évaluations orales pour au mieux nous préparer à de futurs entretiens ou examens.

Les exactes mêmes principes ont été suivis : nous étudions des séries de plus en plus de notions en grammaire anglaise que nous devions savoir retenir et retranscrire à l'examen.

Mais aussi, savoir préparer et soutenir un oral entièrement en anglais, assuré sa grammaire dans celui-ci et répondre aux questions de la classe par la suite.

10

R4.07 Expression Communication 4 (15h)

Enseignant
M. Walter Rohrig

Ayant pour objectif d'améliorer notre communication en entreprise, ce module s'est vu être enrichissant en connaissances théoriques et pratiques pour communiquer plus efficacement. Pour ce faire, nous avons été évalués de manière théorique sur notre compréhension des notions abordées pour au mieux mener une conversation juste avec intérêt, et en pratique sur un atelier de résolution de conflits en entreprise.

L'apprentissage théorique englobait un ensemble de notions comme le droit à l'erreur, la communication interne à l'entreprise comme externe avec des clients, partenaires... mais aussi la gestion du circuit de communication et les prémices de la gestion d'un conflit.

Sur cette dernière notion, nous avons aussi été mis en situation pour gérer un conflit inter sites d'une entreprise. En effet, nous devions avec les tenants d'un conflit trouver un moyen de cerner les attendus pour proposer un plan logique de communication et de gestion du conflit.

11

Annexes

11.1 Résultats d’examens

11.1.1 R4Cyber.11 Sécurisation des services réseaux

IUT des Pays de l'Adour – DUT RT2 FA 2022-2023							
Notes à rendre sur cette liste exclusivement,							
et à remettre directement au secrétariat							
Matière :	R4C11		Date :	10/04/24			
	coeff	1	1	0			
NOMS	Prénoms	QCM	TP		Moyenne	PARCOURS	
ALRIC	LEO-PAUL					ROM	
DAYON	MATHIEU					PILPRO	
DEHU	ALEXIS	12	8.5		10.25	CYBER	
DIENG	Khadim	10.75	9		9.875	CYBER	
EL AKHAL EL BOUZIDI	MOHAMAD	15.33	17		16.165	CYBER	
GORRICHON	MATHIS	11.5	6		8.75	CYBER	
GROLEAU	ANTHONY					PILPRO	
GUIBOREL	TILIO					ROM	
MANAUT	Lilian					ROM	
MARCHAL	ALEXIS					ROM	
MARTIN	BAPTISTE	10	7.5		8.75	CYBER	
MOTZ	MARTIN	9.58	11		10.29	CYBER	
PETIGAS	ROMEO	10.58	8		9.29	CYBER	
PICABIA	ANTTON					PILPRO	
RECART	ANDONI	13.25	11.00		12.125	CYBER	
SAUVAGE	CORENTIN	9.58	5		7.29	CYBER	
	MOY	11.39666667	9.222222222		10.30944444		

11.1.2 R4.03 Physique des télécoms

IUT des Pays de l'Adour – BUT RT2 FA 2023-2024						
Notes à rendre sur cette liste exclusivement,						
et à remettre directement au secrétariat						
Matière :403 Physique des télécoms			Date : mars 2024			
	coeff	6	1	1	1	
NOMS	Prénoms	Théorique	TP1	TP2	TP3	Moyenne
ALRIC	LEO-PAUL	2	9	8	10	4.33
DAYON	MATHIEU	3	14	5	5	4.67
DEHU	ALEXIS	5	15	15	16	8.44
DIENG	Khadim	8.5	10	12	12	9.44
EL AKHAL EL BOUZIDI	MOHAMAD	6	7	2	5	5.56
GORRICHON	MATHIS	1	8	14	8	4.00
GROLEAU	ANTHONY	6	15	8	12	7.89
GUIBOREL	TILIO	8.5	10	8	8	8.56
MANAUT	Lilian	1	8	12	8	3.78
MARCHAL	ALEXIS	6	9	14	14	8.11
MARTIN	BAPTISTE	8	8	16	5	8.56
MOTZ	MARTIN	4	15	17	12	7.56
PETIGAS	ROMEO	2	5	10	2	3.22
PICABIA	ANTTON	5	12	12	5	6.56
RECART	ANDONI	3.00	10.00	12.00	10.00	5.56
SAUVAGE	CORENTIN	1	8	8	5	3.00
	MOY					0.00

11.1.3 R4.05 Automatisation des tâches d'administration

IUT des Pays de l'Adour – DUT RT2 FA 2022-2023								
Notes à rendre sur cette liste exclusivement,								
et à remettre directement au secrétariat								
Matière :R405			Date : 4/5/2024					
	coeff	3	1	0				
NOMS	Prénoms	Note1	Note2	Note3	Moyenne	PARCOURS		
ALRIC	LEO-PAUL	10.29	13.5		11.0925	ROM		
DAYON	MATHIEU	10.21	10.21		10.21	PILPRO		
DEHU	ALEXIS	16.47	16.47		16.47	CYBER		
DIENG	Khadim	13.37	13.37		13.37	CYBER		
EL AKHAL EL BOUZIDI	MOHAMAD	13.95	13.95		13.95	CYBER		
GORRICHON	MATHIS	12.25	12.5		12.3125	CYBER		
GROLEAU	ANTHONY	10.78	11.5		10.96	PILPRO		
GUIBOREL	TILIO	10.67	13.5		11.3775	ROM		
MANAUT	Lilian	6.62	7		6.715	ROM		
MARCHAL	ALEXIS	7.68	10		8.26	ROM		
MARTIN	BAPTISTE	14.23	14.23		14.23	CYBER		
MOTZ	MARTIN	14.89	14.89		14.89	CYBER		
PETIGAS	ROMEO	14.88	14.88		14.88	CYBER		
PICABIA	ANTTON	8.92	12		9.69	PILPRO		
RECART	ANDONI	8.41	11.00		9.0575	CYBER		
SAUVAGE	CORENTIN	0	10		2.5	CYBER		
	MOY	10.85125	12.4375	#DIV/0!	11.2478125			