MINISTERE DES ARMEES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONCOURS

Pour l'accès à l'emploi de contrôleur spécialisé de classe normale

ANNALES

Sessions 2017

ÉPREUVES D'ADMISSIBILITÉ

1ère ÉPREUVE D'ADMISSIBILITE

Epreuve commune aux deux concours

Une épreuve de cas pratique avec une mise en situation à partir d'un dossier à caractère technique remis au candidat pouvant comporter des graphiques ainsi que des données chiffrées.

Le dossier doit relever d'une problématique relative aux politiques publiques et comporter plusieurs questions précédées d'une présentation détaillée destinée à mettre le candidat en situation de travail.

(Durée : 3 heures ; coefficient 3)

EPREUVE DE CAS PRATIQUE :

Contrôleur spécialisé, vous êtes détaché à la préfecture du Val-de-Marne, à Créteil, au cabinet du préfet.

Le directeur du cabinet vous demande, à partir des documents joints, de rédiger, pour le préfet, une fiche de synthèse faisant le point sur les soupçons de menaces cybernétiques étrangères (potentiellement d'origine étatique) pesant sur la France, récemment évoqués par la presse. Le préfet doit, en effet, assister à une réunion sur ce thème, à la préfecture de région Ile de France, et veut pouvoir disposer d'éléments de contexte et d'évaluation des menaces révélées, sans négliger les aspects pratiques permettant de saisir leur réalité.

Il vous demande également de rédiger une réponse à une question de la Chambre de Commerce et d'Industrie du Val-de-Marne, qui sollicite une courte présentation de l'organisation des moyens dont dispose la France pour se protéger contre ces cyberattaques.

De l'armée américaine à Sony, neuf ans de révélations par WikiLeaks

Le Figaro, par Lucie Ronfaut, Jamal El Hassani Mis à jour le 24/06/2015 à 19:13

L'organisation s'est illustrée ces dernières années en publiant des milliers de documents confidentiels appartenant aux autorités américaines. Retour sur ses plus grandes révélations.

Les révélations de la mise sur écoute de trois présidents français par les États-Unis n'auraient pas été possibles sans un acteur bien connu du Web: WikiLeaks. Cette organisation a officiellement pour but de «donner au public les informations les plus importantes». Pour ce faire, elle a recours aux «leaks» («fuites» en français), c'est-à-dire la publication d'un très grand nombre de documents confidentiels sur son site internet. WikiLeaks s'associe aussi régulièrement avec des journaux du monde entier afin de garantir une couverture médiatique à ses révélations. L'organisation est dirigée par son cofondateur, Julian Assange. Ce dernier vit depuis trois ans en exil au sein de l'ambassade d'Équateur à Londres pour échapper à une procédure d'extradition en Suède pour viol.

Fondée en 2006, WikiLeaks s'est fait connaître du grand public quatre ans plus tard grâce à ses révélations sur les guerres en Irak et en Afghanistan. Le site s'est depuis fait plus discret, s'illustrant dernièrement par la publication d'emails piratés à Sony Pictures. L'organisation a aussi brièvement aidé Edward Snowden, qui a permis les révélations des dessous de la NSA, lorsqu'il a fui Hong Kong.

• Les Warlogs

En juillet 2010, WikiLeaks s'est associé à plusieurs journaux pour publier plus de 90.000 fichiers documentant la guerre en Afghanistan menée par les États-Unis entre 2004 et 2009. Ils ont notamment relevé la dissimulation de nombreuses victimes civiles par l'armée américaine. En octobre 2010, ce sont près de 400.000 documents concernant la guerre en Irak qui ont eux aussi été publiés en ligne, révélant la torture et la mort de milliers de civils par les autorités irakiennes, sans réaction de la part des soldats américains sur place.

• Le Cablegate

En novembre 2010, WikiLeaks a commencé à publier une centaine de mémos diplomatiques, provenant d'une base de données de plus de 250.000 documents, de nouveau en partenariat avec plusieurs médias. Ces fichiers traitaient des relations politiques entre certains pays, d'affaires intérieures ou simplement de potins sur des femmes ou des hommes politiques éminents. La publication des Warlogs et du Cablegate a été permise

grâce à Chelsea Manning, ancienne soldate américaine, qui purge aujourd'hui une peine de prison de 35 ans après avoir transmis des centaines de milliers de documents confidentiels à WikiLeaks.

• Les Spy Files

Un an et demi avant les révélations d'Edward Snowden sur les pratiques de la NSA, WikiLeaks alertait le monde sur «la surveillance de masse». «C'est devenu depuis dix ans une industrie internationale qui vend ses services aux dictateurs pour espionner des populations entières», accusait alors Julian Assange. Son site a publié en 2011 plus de 280 documents mettant en cause 160 entreprises, majoritairement occidentales, qui auraient aidé 25 pays considérés comme autoritaires ou dictatoriaux à surveiller leurs citoyens. Parmi les clients: la Chine, l'Iran ou la Syrie. L'affaire est gênante pour des pays comme la France, l'Allemagne, ou Le Royaume-Uni, d'où viennent ces entreprises. Alors que les outils de surveillance de ces sociétés sont souvent interdits dans leurs pays d'origine, ils sont vendus à des régimes qui s'en servent pour traquer leurs opposants.

• The Sony Archives

Fin novembre 2015, Sony Pictures, la filiale américaine dédiée au divertissement du géant de l'électronique japonais, a été la victime d'une importante cyberattaque. Les Américains ont vite accusé la Corée du Nord, qui aurait agi en représailles à la sortie imminente de *The Interview*, un film de Sony Pictures tournant en dérision le régime nord-coréen. Des données confidentielles siphonnées par les hackeurs dans les serveurs de Sony ont fuité sur Internet, y compris des films pas encore sortis. En avril dernier, WikiLeaks a finalement publié «The Sony Archives», une base de données accompagnée d'un moteur de recherche, qui indexe 173.132 e-mails, 30.287 documents et plus de 2200 adresses électroniques de l'entreprise. Le 18 Juin, 276.000 nouveaux documents ont été publiés sur la plateforme.

Le Figaro, 24/06/2015

Le Monde Informatique (LMI)

La France crée un commandement cyberdéfense

Dominique Filippone , publié le 13 décembre 2016

Le ministre de la défense, Jean-Yves Le Drian, a annoncé la création d'un commandement de cyberdéfense afin de répondre aux enjeux de cybersécurité au plus haut niveau de l'Etat. Outre la nomination d'un général quatre étoiles placé sous l'autorité directe du chef d'état-major des Armées, 2 600 militaires spécialisés seront déployés d'ici 2019 sur l'ensemble du territoire épaulés par 4 400 réservistes en cybersécurité.

Afin de lutter le plus efficacement possible contre les cyberattaques, la France semble décidée à mettre le paquet. Profitant de sa visite du pôle d'excellence cyber (PEC) à Bruz en Bretagne, le ministre de la Défense Jean-Yves Le Drian a annoncé la création d'un commandement dédié à la cyberdéfense qui va disposer de moyens jusqu'alors inédits.

« L'émergence d'un nouveau milieu, le cyber, doit nous amener à repenser profondément notre manière d'aborder l'art de la guerre », a indiqué Jean-Yves Le Drian. « Nos capacités cyber offensives doivent nous permettre de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives ».

2 600 combattants numériques déployés en 2019

Cela passe notamment par la création d'un poste de commandeur (Cybercom), un officier général 4 étoiles, dont la mission va être de mener à bien les opérations militaires dans « l'espace numérique ». Un état-major à part entière est également créé, constitué de 2 600 militaires appelés « combattants du numérique » placés sous la direction du commandeur qui répondra directement au chef d'état-major des armées.

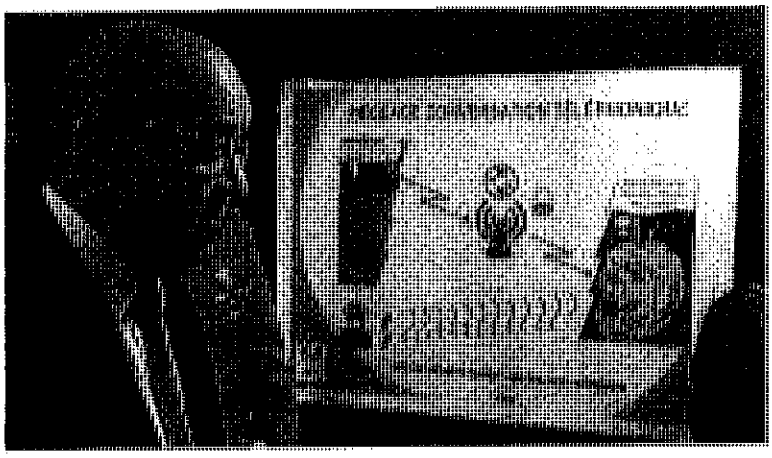
Le déploiement de cette force en cyberdéfense est prévue en 2019, renforcé par la mobilisation autant que de besoin de 4 400 réservistes en cybersécurité. Par ailleurs, il est prévu que plus de 400 personnes au sein de la direction générale de l'armement (DGA) Maîtrise de l'information à Bruz soient également mobilisées, sachant qu'à terme ils pourraient être 200 de plus à travailler sur la problématique de la protection des réseaux.

Article rédigé par Dominique Filippone, Chef des actualités LMI

Le ministère de la Défense a déjoué 24.000 cyberattaques en 2016

Par lefigaro.fr

Publié le 08/01/2017 à 12:08



Après le piratage informatique intervenu dans la présidentielle américaine, Jean-Yves Le Drian confirme que la France est également victime de ce type d'assauts numériques. Il appelle à la vigilance à quelques mois de la présidentielle.

À moins de 4 mois de la présidentielle, la révélation a de quoi susciter des inquiétudes. Alors que les renseignements américains dénoncent l'attaque russe contre le parti démocrate lors de la dernière élection présidentielle, le ministre de la Défense, Jean-Yves Le Drian, révèle que la France n'est pas épargnée par la menace.

Bien au contraire, il faudrait même être «naïf» pour le croire, selon le ministre, qui explique dans le *Journal du dimanche*, que «la menace cybernétique est devenue majeure» depuis trois ans «y compris sur nos propres outils militaires». «Les tentatives d'agressions informatiques sur mon ministère doublent chaque année. En 2016, 24.000 attaques externes ont été bloquées par nos dispositifs de sécurité. Parmi celles-ci, quelques centaines, plutôt élaborées, avaient de véritables intentions de nuire.» Il cite par exemple «des tentatives d'atteinte à l'image du ministère, des attaques menées à des fins stratégiques (harcèlement, repérage, espionnage) et même des tentatives de perturbation de nos systèmes de drones».

«Les analyses effectuées par l'Agence nationale de la sécurité des systèmes d'information (Anssi) n'ont pas permis à ce jour d'identifier des indices d'opérations de déstabilisation ciblant» la prochaine élection présidentielle, ajoute Jean-Yves Le Drian au JDD. «Il ne peut cependant être exclu que des opérations de même nature que celles observées aux États-

Unis cherchent à perturber le processus électoral français», prévient-il. «J'appelle donc chacun à la plus grande vigilance.»

Première force cyber européenne

Jean-Yves Le Drian réaffirme que la France doit être capable de contre-attaquer et souhaite ainsi doubler les «combattants numériques» pour arriver à un effectif de 2600 en 2019. Près de 2 milliards d'euros sur 6 ans sont consacrés au sujet. «Cela fait de la France la première force cybereuropéenne au côté des Britanniques.»

Les États-Unis, eux, sont en plein mélodrame depuis que le FBI, la CIA et la NSA ont accusé la Russie d'avoir organisé une attaque informatique contre les démocrates de manière à discréditer Hillary Clinton et à favoriser l'élection de Donald Trump. La partie du rapport rendu public vendredi désigne même nommément le président russe, Vladimir Poutine, comme le donneur d'ordre de cette attaque. Le rapport émet un avertissement glaçant: Moscou «appliquera les leçons apprises» dans cette campagne pour influencer les élections dans d'autres pays.

Jean-Yves Le Drian révèle au *JDD* que les responsables des principaux mouvements politiques ont été reçus par l'Anssi afin d'éviter qu'un scénario à l'américaine ne se déroule dans les prochains mois. Mais comme le dit l'adage, le risque zéro n'existe pas.

ASSEMBLÉE NATIONALE

14ème législature

Question N° : 4688	De M. Olivier Falorni (Radical, républicain, démocrate et progressiste - Charente-Maritime)	Question au gouvernement
Ministère interrogé > Affaires étrangères	**Ministère attributaire** > Affaires étrangères	
Rubrique >télécommunications	**Tête d'analyse** >Internet	**Analyse** > cybercriminalité. lutte et prévention.
Question publiée au JO le : **16/02/2017** Réponse publiée au JO le : **16/02/2017** page : **1024**		

Texte de la question

Texte de la réponse

LUTTE CONTRE LES CYBERATTAQUES

M. le président. La parole est à M. Olivier Falorni, pour le groupe radical, républicain, démocrate et progressiste.

M. Olivier Falorni. Monsieur le ministre des affaires étrangères, l'invasion du tout numérique a rendu notre société tributaire des systèmes d'information et de communication. Dans ce cadre, l'essor du monde numérique s'est accompagné d'un développement des menaces liées à de nouvelles formes de criminalité. Je pense notamment aux modes d'action cachés de la cyberguerre ou du cyberespionnage économique.

Récemment, le renseignement américain a confirmé que des *hackers* russes étaient intervenus dans l'élection américaine pour affaiblir la candidature d'Hillary Clinton. La France n'est pas épargnée par la menace. Près de 24 000 attaques informatiques ont été bloquées en 2016 par les dispositifs de sécurité nationaux. À l'approche de l'élection présidentielle, des piratages informatiques et une cyberdéstabilisation sont déjà à l'œuvre.

Ces attaques sont organisées et coordonnées par un groupe structuré qui pirate des milliers de documents et qui les fait publier par le site Wikileaks. Parallèlement, des informations calomnieuses de sites étrangers, pour la plupart russes, sont massivement relayées sans aucun filtre sur les réseaux sociaux.

Ces faits sont graves. Une puissance étrangère ne peut saper une élection démocratique, libre et équitable. Dès lors, il faut que les conditions de sécurité soient assurées contre les cyberattaques et ingérences afin de garantir le déroulement normal de ce scrutin.

À cette fin, un conseil de défense s'est réuni ce matin en présence du Président de la République. Monsieur le ministre, quelles mesures spécifiques de vigilance et de protection ont été prises face à ces menaces très importantes ? *(Applaudissements sur les bancs du groupe radical, républicain, démocrate et progressiste.)*

M. Dominique Raimbourg et M. François de Rugy. Très bien !

7/20

ASSEMBLÉE NATIONALE

M. le président. La parole est à M. le ministre des affaires étrangères et du développement international.

M. Jean-Marc Ayrault, *ministre des affaires étrangères et du développement international.* Monsieur le député, vous avez parfaitement raison d'évoquer ce point essentiel. Après ce qui s'est passé aux États-Unis, il est en effet de notre responsabilité de prendre toutes les mesures pour que l'intégrité de notre processus démocratique soit pleinement respectée ; telle est la volonté du Gouvernement.

Je l'affirme haut et fort : la non-ingérence dans les affaires intérieures d'un autre État est un principe cardinal de la vie internationale. Nous n'accepterons pas quelque ingérence que ce soit dans notre processus électoral, pas plus de la Russie que de tout autre État. Il y va de notre démocratie, il y va de notre souveraineté, il y va de notre indépendance nationale.

Que devons-nous faire ? Nous devons d'abord être vigilants sur tout ce qui relève de la désinformation des organes de presse qui sont parfois étroitement liés à des États tiers. Ensuite, nous devons faire clairement connaître les limites à ceux qui seraient tentés de porter atteinte au principe de non-ingérence, y compris en prenant des mesures de rétorsion si nécessaire.

M. Claude Goasguen. Comment ?

M. Jean-Marc Ayrault, *ministre.* En effet, aucun État étranger ne peut influencer le choix des Français. Aucun État étranger ne peut choisir le futur Président de la République. Et je souhaiterais que les candidats ou candidates qui se voient assurés d'une préférence par un État, en particulier s'il s'agit d'un pays que l'on connaît bien, la Russie, se révoltent contre ce type d'influence.

M. Claude Goasguen. Macron ?

M. Jean-Marc Ayrault, *ministre.* Pour l'heure, je ne les ai pas entendus.

M. Claude Goasguen. Parce que ce n'est pas prouvé !

M. Jean-Marc Ayrault, *ministre.* En tout cas, la position du Gouvernement est claire. Nous avons évoqué le sujet ce matin en conseil de défense, mais une séance exceptionnelle sera dédiée la semaine prochaine au renforcement des mesures qui ont déjà été prises contre les cyberattaques.

L'Agence nationale de la sécurité des systèmes d'information est à la disposition des partis politiques et des candidats pour les conseiller. Nous prendrons d'autres mesures que nous vous annoncerons pour garantir l'intégrité de cette consultation populaire. *(Applaudissements sur les bancs du groupe socialiste, écologiste et républicain et du groupe radical, républicain, démocrate et progressiste.)*

8/20

Espionnage par objets connectés : WikiLeaks révèle des documents de la CIA

Modifié le 08/03/2017 à 13:45 - Publié le 07/03/2017 à 19:10 | AFP

Smartphones, télévisions connectées ou encore logiciels populaires peuvent être transformés en appareils d'écoute à l'insu de leur utilisateur, affirme WikiLeaks ©AFP/Archives / John SAEKI, Laurence CHU AFP

La CIA peut transformer votre télévision en appareil d'écoute, contourner les applications de cryptage voire contrôler votre véhicule, selon des documents publiés mardi par WikiLeaks, qui met en garde contre le risque d'une prolifération des "armes" informatiques ainsi exposées.

WikiLeaks a publié près de 9.000 documents présentés comme provenant de la CIA, estimant qu'il s'agissait de la plus importante publication de matériels secrets du renseignement jamais réalisée.

Pour le site créé par l'Australien Julian Assange, ces documents prouvent que la CIA opère comme l'agence de sécurité nationale (NSA), principale entité de surveillance électronique des Etats-Unis, mais avec moins de supervision.

Un porte-parole de la CIA, Jonathan Liu, n'a ni confirmé ni démenti l'authenticité de ces documents, ni commenté leur contenu.

"C'est quelque chose qui n'a pas été entièrement évalué", a déclaré mardi le porte-parole de la Maison Blanche, Sean Spicer, lors de son point de presse.

Pour autant, le président la commission du Renseignement à la Chambre des représentants, Devin Nunes, a affirmé ces révélations semblaient "très très sérieuses". "Nous sommes très inquiets", a-t-il ajouté.

Le site affirme qu'une grande quantité de documents de la CIA mettant au jour "la majorité de son arsenal de piratage informatique" a été diffusée auprès de la communauté de la cyber-sécurité. WikiLeaks en a lui-même reçu une partie qu'il a décidé de rendre publique.

"Ces archives semblent avoir circulé parmi d'anciens pirates du gouvernement américain et sous-traitants de façon non autorisée, l'un d'entre eux ayant fourni à WikiLeaks une partie de ces archives", a précisé le site, qui avait publié en 2010 des centaines de milliers de documents de la diplomatie américaine qui avaient fait trembler les chancelleries du monde entier.

Contrôle

"Cette collection extraordinaire, qui représente plusieurs centaines de millions de lignes de codes, dévoile à son détenteur la totalité de la capacité de piratage informatique de la CIA", avance-t-il.

Si ces documents sont vérifiés, ils pourraient considérablement gêner le renseignement américain, dont l'ampleur du système de surveillance a déjà été largement exposée par l'ancien consultant de la NSA, Edward Snowden, en 2013.

La police a aussi arrêté l'an dernier un autre responsable de la NSA, chez qui elle avait retrouvé des documents classés secrets, datant parfois de 20 ans.

Selon le site, ces documents montrent que l'agence de renseignement a élaboré plus d'un millier de programmes malveillants, virus, cheval de Troie et autres logiciels pouvant infiltrer et prendre le contrôle d'appareils électroniques.

Ces programmes ont pris pour cible des IPhone, des systèmes fonctionnant sous Android (Google) -qui serait toujours utilisé par Donald Trump-, le populaire Microsoft ou encore les télévisions connectées de Samsung, pour les transformer en appareils d'écoute à l'insu de leur utilisateur, affirme WikiLeaks.

La CIA s'est également intéressée à la possibilité de prendre le contrôle de véhicules grâce à leurs instruments électroniques.

En piratant les smartphones, relève le site, la CIA parviendrait ainsi à contourner les protections par cryptage d'applications à succès comme WhatsApp, Signal, Telegram, Weibo ou encore Confide, en capturant les communications avant qu'elles ne soient cryptées.

Imprudence

"De nombreuses vulnérabilités exploitées par le cyber-arsenal de la CIA sont omniprésentes et certaines peuvent déjà avoir été découvertes par des agences de renseignement rivales ou par des cybercriminels", met en garde WikiLeaks.

Dans un communiqué, Julian Assange estime que ces documents prouvent des "risques extrêmes" induits par la prolifération hors de toute supervision des "armes" de cyberattaque, sans même avertir les fabricants des appareils visés.

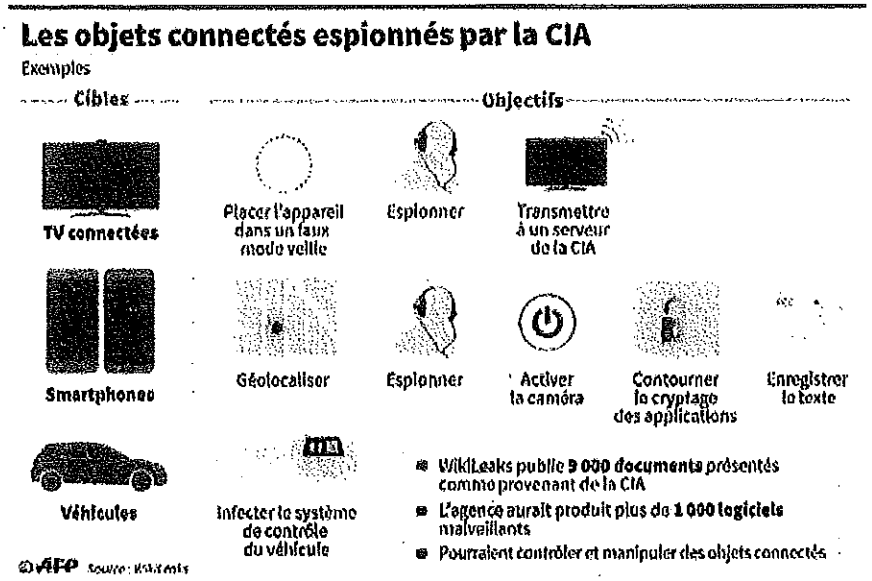
Edward Snowden a affirmé sur Twitter que ces documents semblaient "authentiques".

Mais le fait d'exploiter des failles est "imprudent au-delà des mots", estime M. Snowden. "Parce que n'importe quel pirate informatique peut se servir de ces vulnérabilités mises au jour par la CIA pour s'introduire dans n'importe quel iPhone dans le monde".

La directrice générale de l'association Electronic Frontier Foundation, Cindy Cohn, reproche à la CIA de n'avoir pas aidé à combler les lacunes de sécurité des appareils visés.

AFP, 08 03 2017

10/20



"Ces fuites montrent que nous sommes moins en sécurité avec la CIA quand elle décide de laisser en l'état les failles, plutôt que de les combler", a-t-elle estimé.

Cette affaire est d'autant plus embarrassante pour la CIA qu'elle fait partie des agences qui avaient conclu en octobre que la Russie avait interféré dans la campagne présidentielle américaine, en piratant justement le parti démocrate puis en diffusant, par l'intermédiaire de WikiLeaks, des emails d'un proche conseiller d'Hillary Clinton.

La célèbre agence est par ailleurs accusée par Donald Trump, comme les autres agences de renseignement, de faire fuiter des informations suggérant que certains de ses proches ont eu des contacts l'an dernier avec le renseignement russe.

08/03/2017 13:35:15 - Washington (AFP) -

euronews. **08 mars 2017**

Apple annonce avoir déjà colmaté la plupart des brèches de sécurité de ses appareils, tandis que Samsung a dit se pencher "urgemment" sur la question.
Embarrassantes pour ces géants de l'électronique, les révélations de WikiLeaks selon lesquelles la CIA peut transformer votre téléphone ou votre téléviseur en appareil d'écoute, contourner les applications de cryptage, voire contrôler votre véhicule, ont frappé comme un nouveau coup de tonnerre.

C'est mardi 7 mars que WikiLeaks a publié des milliers de documents présentés comme provenant de l'agence américaine de renseignement.

Baptisé "Vault 7", le rapport de WikiLeaks prévoit une série de fuites, la plus importante de l'histoire.

La première partie, appelée "Year Zero" concerne 8 761 documents qui auraient été obtenus depuis un réseau ultra-sécurisé situé à l'intérieur du siège de la CIA, en Virginie. Des documents qui montrent que la CIA a élaboré plus d'un millier de programmes malveillants, virus, chevaux de Troie,..., pouvant infiltrer et contrôler les iPhone d'Apple, des systèmes fonctionnant sous Androïd de Google, Windows de Microsoft, des appareils Samsung...

Le consulat américain à Francfort aurait également servi de base aux hackers de la CIA pour couvrir l'Europe, le Moyen Orient et l'Afrique.

Pour l'expert en sécurité numérique Will Donaldson, PDG de Nomx, il n'y a rien d'étonnant, mais il faut agir :

"Ils écoutent dans les voitures, ils écoutent par le biais de vos téléviseurs. Ils écoutent par n'importe quel appareil qui possède une batterie basiquement. C'est pour cela que c'est si répandu, il y a tellement de trous. Nous commençons juste à regarder. Je pense que Samsung fait partie des marques qui ont des manquements en matière de sécurité et qu'ils ont listées, ils peuvent les allumer à distance sans que cela se voit. N'importe qui ici dans cette pièce pourrait être surveillé sans le savoir ou le vouloir."

En piratant les smartphones, la CIA parviendrait aussi à contourner les protections par cryptage d'applications à succès comme WhatsApp, Signal, Telegram, Weibo ou encore Confide, en captant les communications avant qu'elles ne soient cryptées.

"Je pense que tout ce qui est connecté à internet est piratable, c'est quelque chose qui peut être compromis, au final vous devez être attentif, savoir où vous voulez que vos appareils soient placés dans vos maisons, vos bureaux, quelles places leur donner dans votre vie personnelle", explique encore l'expert en cybersécurité, Varun Badhwar, PDG de RedLock.

Pour le site créé par l'Australien Julian Assange, tous ces documents prouvent que la CIA opère comme la NSA, la principale entité de surveillance électronique des Etats-Unis, mais avec moins de supervision : un danger selon lui qui critique les "risques extrêmes" induits par la prolifération non supervisée des "armes" de cyberattaque, sans même avertir les fabricants des appareils visés.

Wikileaks : 5 questions pour comprendre les dernières révélations

Le site de Julian Assange a mis en ligne plus de 8.000 documents internes de la CIA décrivant les techniques utilisées par l'agence pour pirater des smartphones et des télévisions connectées.

Wikileaks a publié des milliers de documents mettant en cause la CIA Crédit : AFP

Benjamin Hue *Journaliste RTL*

PUBLIÉ LE 09/03/2017 À 09:28 MIS À JOUR LE 09/03/2017 À 18:00

Près de quatre ans après les révélations d'Edward Snowden sur la NSA, les petits secrets du renseignement américain sont à nouveau étalés sur la place publique. Mardi 7 mars, l'organisation Wikileaks a mis en ligne plusieurs milliers de documents internes détaillant plusieurs dizaines de programmes d'espionnage électronique de la CIA. Baptisée "Vault 7", cette publication est présentée comme la plus importante fuite de documents confidentiels de l'histoire de l'agence du renseignement extérieur américain. Wikileaks affirme détenir des informations sur plus de 500 programmes au total et promet de les publier dans les prochaines semaines.

La première partie, **"Year Zero", compile près de 9.000 fichiers** couvrant une période s'étalant de 2013 à 2016. Elle met à nu les capacités d'espionnage de la CIA et le recours **à des pratiques particulièrement intrusives.** Selon ces documents, la CIA aurait employé de nombreux ingénieurs et hackers pour élaborer des milliers de logiciels malveillants et développer un arsenal technologique capable aussi bien de transformer des télévisions et voitures connectés en mouchards, d'espionner des iPhone et des smartphones Android ou encore de contourner des antivirus commerciaux.

1 - Ces documents sont-ils authentiques ?

Ces milliers de documents doivent encore être analysés par des experts et des journalistes. Mais plusieurs spécialistes du renseignement les jugent d'ores et déjà authentiques. "Je suis encore plongé dans cette publication mais ce que Wikileaks a sorti est réellement important. Et paraît authentique", a tweeté Edward Snowden mardi soir. Ces révélations doivent également être nuancées à la lumière de la nature de Wikileaks, une ONG militant pour la transparence se réclamant d'une promesse de neutralité que ses détracteurs voient au contraire comme un acteur géostratégique à la solde du Kremlin depuis l'affaire des emails qui a empoisonné la campagne présidentielle d'Hillary Clinton.

Sans surprise, **la CIA n'a pas confirmé l'authenticité des données publiées par Wikileaks**. Dans un communiqué, l'agence américaine a rappelé les grandes lignes de sa mission, à savoir "collecter activement des renseignements afin de protéger l'Amérique des terroristes, des nations hostiles et d'autres adversaires". Une porte-parole de la CIA a quant à elle accusé Wikileaks d'œuvrer pour les adversaires des États-Unis en révélant ses méthodes.

2 - Quelles sont les techniques révélées ?

Plus qu'elle ne révèle la capacité de la CIA à pénétrer dans des appareils électroniques, "Vault 7, Year Zero" détaille les méthodes utilisées par l'agence dans cette perspective. Parmi les outils les plus marquants, "Weeping Angel", développé en partenariat avec le MI5 britannique, permet de **transformer des téléviseurs connectés Samsung en espion** pour enregistrer des sons à proximité et les transmettre à des serveurs distants alors que le poste semble hors-tension. L'agence aurait également développé **des logiciels d'espionnage capables de contourner la protection des antivirus commerciaux** afin de copier le contenu d'un disque dur.

Plusieurs programmes décrivent comment la CIA a mis au point **des logiciels espions pour infecter des iPhone** et accéder à distance à la géolocalisation, aux SMS, aux conversations, à la caméra et au micro de la cible. Wikileaks affirme également que la CIA a eu connaissance de 24 failles 0day - non documentées et pas encore corrigées - lui permettant d'espionner des appareils Android. Plus largement, l'agence aurait tenu à jour un vaste catalogue de failles de sécurité - achetées ou transmises par des agences amies - pour les maintenir au mépris de la sécurité des utilisateurs.

3 - Les consommateurs sont-ils concernés ?

Contrairement aux programmes secrets de surveillance de masse développés par la NSA et révélés par Edward Snowden en 2013, ceux de la CIA semblent relever de l'espionnage ciblé. Ces armes numériques sont vraisemblablement utilisées pour suivre les activités de suspects ou d'entreprises. Les documents indiquent que **la plupart d'entre elles nécessitent d'ailleurs un accès physique à la machine visée**. La CIA ne peut pas transformer un téléviseur connecté en machine de surveillance à distance. Elle doit accéder au domicile de la cible

pour l'installer via un port USB. Elle ne peut pas non plus installer de logiciel espion pour IPhone et smartphones Android sans mettre la main dessus. Et les logiciels servant à tromper les antivirus doivent être installés à partir d'un CD ou d'un DVD vierge.

4 - Les messageries chiffrées sont-elles compromises ?

Plusieurs médias américains ont affirmé dans la foulée de la publication des documents que la CIA avait la capacité de contourner le chiffrement de services de messagerie comme WhatsApp, Signal ou Telegram et d'accéder au contenu de leurs messages. En réalité, il semble que **la CIA n'a pas réussi à casser le chiffrement de ces applications**. Les techniques décrites dans "Vault 7, Year Zero" permettent de collecter les messages et d'espionner les communications avant qu'ils ne soient chiffrés. La CIA est en fait parvenue à percer les systèmes d'exploitation sur lesquels sont installées ces applications chiffrées.

"Les révélations de Wikileaks portent sur des logiciels malveillants infiltrés dans des téléphones et pas sur un contournement du protocole de chiffrement de Signal", a réagi mardi Open Whisper Systems, qui développe l'application Signal. "Il est incorrect de dire que la CIA a piraté ces applications et leur chiffrement. Mais les documents montrent qu'IOS et Android ont été piratés, ce qui est un problème beaucoup plus important", a souligné de son côté Edward Snowden.

5 - Quel risque pour les citoyens ?

À ce stade des révélations, le principal écueil pour les citoyens "normaux" se situe du côté des failles de sécurité et des portes dérobées délibérément entretenues et non corrigées par la CIA. Il existe **un risque qu'elles tombent entre de mauvaises mains** et mettent en péril la sécurité informatique de millions d'utilisateurs. Après l'affaire Snowden, les agences de renseignement s'étaient pourtant engagées à communiquer plus rapidement les failles de sécurité qu'elles mettent au jour aux constructeurs de produits et logiciels technologiques.

Les documents mis en ligne listent notamment 14 failles de sécurité permettant de tracer et d'espionner les utilisateurs d'iPhone. Apple a réagi en affirmant que la dernière mise à jour de son logiciel IOS avait corrigé la plupart de ces vulnérabilités et que pratiquement 80% des utilisateurs l'avaient déjà téléchargée. Les autres - les utilisateurs d'iPhone et d'iPad utilisant d'anciennes versions d'iOS qui ne sont plus éligibles aux mises à jour de la marque - courent le risque que ces brèches soient exploitées un jour.

La donne est plus compliquée pour les utilisateurs de smartphones Android, qui fournissent 80% du parc mondial d'appareils. Chaque constructeur doit adapter les mises à jour déployées par Google à ses propres produits, qui fonctionnent avec une version légèrement modifiée du logiciel, ce qui nécessite un délai supplémentaire. Et la plupart des modèles d'entrée de gamme ne tournent tout simplement pas avec la dernière version du logiciel.

RTL, 9 mars 2017

15/20

Pour le patron de la CIA, WikiLeaks est un "service de renseignement hostile"

Le directeur de l'agence de renseignement américaine a estimé que le site de Julian Assange représentait une menace pour les démocraties et faisait le jeu des dictateurs.

Le directeur de la CIA Mike Pompeo lors d'une conférence du Center for Strategic and International Studies à Washington (Etats-Unis), le 13 avril 2017. (CHIP SOMODEVILLA / GETTY IMAGES NORTH AMERICA / AFP)

franceinfo avec AFPFrance Télévisions

Mis à jour le 14/04/2017 | 08:55
publié le 14/04/2017 | 08:19

Le directeur de la CIA ne voit pas le site WikiLeaks d'un bon œil. Mike Pompeo, nommé en février à la tête de l'agence de renseignement américaine, a affirmé jeudi 13 avril que le site de Julian Assange était l'une des principales menaces que les Etats-Unis doivent affronter. *"WikiLeaks se comporte comme un service de renseignement hostile et s'exprime comme un service de renseignement hostile"*, a-t-il assuré devant le Center for Strategic and International Studies, un groupe de réflexion installé à Washington. *"Il a incité ses partisans à intégrer la CIA de façon à obtenir des informations."*

"Assange fait cause commune avec les dictateurs"

Le site *"se concentre de manière écrasante sur les Etats-Unis, tout en cherchant le soutien de pays et d'organisations antidémocratiques"*, a poursuivi Mike Pompeo. WikiLeaks a récemment publié des documents confidentiels révélant les techniques de piratage informatique de la CIA. Il a également mis en ligne, en 2010, 251 000 correspondances d'ambassades américaines classifiées. Le site fondé par Julian Assange a aussi dévoilé des documents du parti démocrate en pleine campagne présidentielle, portant un coup à la campagne d'Hillary Clinton.

"[Julian] *Assange et ses pairs font aujourd'hui cause commune avec les dictateurs. Bien sûr, ils essaient en vain de se draper eux-mêmes et leurs actions dans une démarche de protection de la liberté et de la vie privée,* a estimé le patron de la CIA. *En réalité, ils ne défendent rien d'autre que leur célébrité. Leur monnaie, c'est la course au clic. Leur sens de la morale est inexistant."*

AFP-France Info, 14/04/2017

16/20

ANSSI
Agence nationale de la sécurité des systèmes d'information

LA SSI EN FRANCE

Comme le précise la loi n°2013-1168 du 18 décembre 2013, « le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information », l'ANSSI, rattachée au secrétaire général de la défense et de la sécurité nationale.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 (Journal officiel du 8 juillet 2009), sous la forme d'un service à compétence nationale.

L'ANSSI s'est substituée à la direction centrale de la sécurité des systèmes d'information (DCSSI) du secrétariat général de la défense nationale (SGDN) tout en en renforçant les compétences, les effectifs et les moyens.

Autorité nationale en matière de sécurité et de défense des systèmes d'information, l'ANSSI constitue un réservoir de compétences qui met son expertise et assiste les administrations et les opérateurs d'importance vitale.
Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux. Elle contribue au développement de la confiance dans le numérique.
Le centre de transmission gouvernemental, placé sous l'autorité du SGDSN, assiste l'ANSSI à travers la mise en œuvre les moyens sécurisés de commandement et de liaison nécessaires au président de la République et au Gouvernement

Conformément aux orientations du livre blanc sur la défense et la sécurité nationale 2013, l'ANSSI contribue à l'orientation de la recherche nationale et européenne en matière de sécurité des systèmes d'information.

ANSSI, site officiel, SSI, consultation : avril 2017

17/20

En tant que de besoin, l'ANSSI bénéficie de l'expertise d'un comité stratégique constitué de responsables de haut niveau de l'administration. La mission de ce comité est de proposer la stratégie de l'État en la matière.

Son directeur général, Guillaume Poupard, a été nommé par décret en date du 27 mars 2014.

Évolution de la SSI

La Loi de programmation militaire promulguée le 19 décembre 2013 a renforcé les missions de l'ANSSI. Son article 22 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale et confère à l'ANSSI de nouvelles prérogatives : au nom du Premier ministre elle pourra imposer aux OIV des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques. De plus, l'article 22 rend obligatoire la déclaration des incidents constatés par les OIV sur ces systèmes.

La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques

La Stratégie nationale pour la sécurité du numérique, dévoilée ce 16 octobre 2015 par Monsieur le Premier ministre Manuel Valls, est destinée à accompagner la transition numérique de la société française.

Elle a fait l'objet de travaux interministériels coordonnés par l'ANSSI.

Elle répond aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liées avec cinq objectifs :

- Garantir la souveraineté nationale
- Apporter une réponse forte contre les actes de cybermalveillance
- Informer le grand public
- Faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises
- Renforcer la voix de la France à l'international.

Avec la Stratégie nationale pour la sécurité du numérique, l'Etat s'engage au bénéfice de la sécurité des systèmes d'information pour aller, par une réponse collective, vers la confiance numérique propice à la stabilité de l'État, au développement économique et à la protection des citoyens.

ANSSI, site officiel, SSI, consultation : avril 2017

18/20

La sécurité des systèmes d'information (SSI) et le Livre blanc sur la défense et la sécurité nationale de 2008

Ce Livre blanc, retenant le risque d'une attaque informatique contre les infrastructures nationales comme l'une des menaces majeures les plus probables des quinze prochaines années, mettait en exergue l'impact potentiellement très fort de telles attaques sur la vie de la nation. Notre dépendance aux processus informatiques croît en effet sans cesse avec le développement de la société de l'information et l'utilisation de plus en plus poussée de l'informatique dans les processus essentiels de l'État et de la société.
En conséquence, le Livre blanc invitait l'État à se doter d'une capacité de prévention et de réaction aux attaques informatiques, et à en faire une priorité majeure de son dispositif de sécurité nationale. En particulier, dans le domaine de la défense des systèmes d'information, il soulignait la nécessité de disposer d'une capacité de détection précoce des attaques informatiques, et d'une organisation propre à contrer les attaques les plus subtiles comme les plus massives. Dans le domaine de la prévention, il proposait un recours accru à des produits et à des réseaux de haut niveau de sécurité, et la mise en place d'un réservoir de compétences au profit des administrations et des opérateurs d'infrastructures vitales.
L'ANSSI a été créée conformément aux orientations de ce Livre blanc sur la défense et la sécurité nationale. Afin de proposer la stratégie nationale en matière de sécurité des systèmes d'information, un comité stratégique de la SSI a été institué par le décret portant création de l'ANSSI.
En complément de la création de l'ANSSI, ce Livre blanc a prévu la mise en place au niveau de chaque zone de défense et de sécurité d'un observatoire zonal de la sécurité des systèmes d'information (OzSSI). Ces observatoires ont pour mission de relayer, sur l'ensemble du territoire national, les mesures prises pour améliorer la sécurité des systèmes d'information.

Le Livre blanc sur la défense et la sécurité nationale de 2013 & LPM

En 2013, en réponse au constat de l'augmentation en quantité et en sophistication des cyberattaques contre les systèmes d'information de nombreuses entreprises nationales et de l'État, a été publié un nouveau Livre blanc. Il marque un tournant : l'État ne se contente plus de répondre à ses propres besoins en cybersécurité, il prend en compte désormais ceux des opérateurs vitaux pour la nation.

Ce renforcement implique pour les systèmes d'information les plus critiques de ces opérateurs :

- le respect de référentiels de sécurité à appliquer ;
- la mise en place de dispositifs de détection d'attaques adaptés ;

- l'obligation de déclarer les incidents significatifs ;
- la capacité pour l'État de vérifier par des audits le niveau de sécurité de ces systèmes et, en cas de crise grave, d'imposer les mesures nécessaires.

Promulguée le 19 décembre 2013, la loi n°2013-1168 de programmation militaire (LPM) suit les orientations fixées par le Livre blanc sur la défense et la sécurité nationale 2013. Elle constitue l'outil législatif qui va permettre aux opérateurs publics et privés critiques pour la nation de mieux se protéger et à l'ANSSI – et à d'autres services de l'État – de mieux les soutenir en cas d'attaque informatique. Son article 22 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale et confère au Premier ministre de nouvelles prérogatives.

La stratégie SSI

En février 2011, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a rendu publique la Stratégie de la France en matière de défense et de sécurité des systèmes d'information.

Pour se prémunir des attaques informatiques et garantir la sécurité des Français, des entreprises et de la Nation dans le cyberespace, la stratégie française pose quatre objectifs stratégiques :

- être une puissance mondiale de cyberdéfense et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie ;
- garantir la liberté de décision de la France par la protection de l'information de souveraineté ;
- renforcer la cybersécurité des infrastructures vitales nationales ;
- et assurer la sécurité dans le cyberespace.

Le document présentant ces quatre objectifs stratégiques et les sept axes d'effort qui en découlent permettra à tous les citoyens de comprendre les enjeux et la portée de l'action gouvernementale.

Une nouvelle stratégie de la France, en cours d'élaboration, sera présentée au premier semestre 2015.

La France dispose également d'un réseau de CERT, organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT (Computer Emergency Response Team) sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et/ou aux administrations, mais dont les informations sont généralement accessibles à tous.

ANSSI, site officiel, SSI, consultation : avril 2017

CAS PRATIQUE

COPIE AYANT OBTENU LA MEILLEURE NOTE À CETTE EPREUVE

MINISTÈRE DES ARMÉES

Session de 2017

CONCOURS

Pour l'accès à l'emploi de contrôleur spécialisé de classe normale
Épreuve : *de cas pratique*

Réservé à la notation

15,33 / 20

Sujet :

Contrôleur spécialisé, vous êtes détaché à la préfecture du Val-de-Marne, à Créteil, au cabinet du préfet.

Le directeur du cabinet vous demande, à partir des documents joints, de rédiger, pour le préfet, une fiche de synthèse faisant le point sur les soupçons de menaces cybernétiques étrangères (potentiellement d'origine étatique) pesant sur la France, récemment évoqués par la presse. Le préfet doit, en effet, assister à une réunion sur ce thème, à la préfecture de région Ile de France, et veut pouvoir disposer d'éléments de contexte et d'évaluation des menaces révélées, sans négliger les aspects pratiques permettant de saisir leur réalité.

Il vous demande également de rédiger une réponse à une question de la Chambre de Commerce et d'Industrie du Val-de-Marne, qui sollicite une courte présentation de l'organisation des moyens dont dispose la France pour se protéger contre ces cyberattaques.

I -
Préfecture du Val-de-Marne
Cabinet du préfet

Créteil, le 20 avril 2017

FICHE DE SYNTHESE

Objet : Cyber menaces étrangères : contexte et évaluation de la menace

Alors que les élections présidentielles et législatives françaises se profilent à l'horizon, on ne peut qu'avoir en tête les cas révélés d'ingérences russes dans le processus électoral américain. De plus, le site Wikileaks n'a de cesse de nous prévenir des dangers du développement du numérique sur le respect du secret et de la liberté, notamment avec les révélations récentes des failles de sécurité des objets connectés qui, au lieu d'être signalées pour pouvoir être corrigées, ont été exploitées par les services de renseignements américains.

Concernant les menaces d'ingérence qui pèsent sur le processus électoral français, elles ne sont pas prises à la légère. Le gouvernement est conscient de la menace et a mis en place, lors de conseils de la défense dédiée, dès le mois de février, des mesures visant à endiguer toute forme d'intrusion dans le choix du futur président de la république par les français.

Il a par ailleurs mis à profit l'Agence Nationale de la Sécurité des Systèmes d'Information afin qu'il pré-alerte les différents partis politiques et leurs candidats afin de contrer toute influence étrangère et, garantir la sécurité numérique de leur campagne.

La France n'est pas novice dans le domaine de la cyber sécurité puisque rien qu'en 2016, ce sont près de 240000 attaques externes et tentatives d'intrusion qui ont été bloquées grâce à nos systèmes de cyber sécurité.

Plane également, à l'heure actuelle, la menace d'espionnage industriel et économique par l'intermédiaire des objets connectés qui ont une part de plus en plus importante dans notre vie. Le site Wikileaks a publié, début mars, près de 9000 documents classifiés provenant vraisemblablement de la CIA, dans lesquels seraient répertoriés des milliers de programmes espions ou, virus qui permettraient de détourner nos objets connectés de leur usage initial.

L'ensemble de ces malwares utiliseraient des failles logicielles identifiées par la CIA et donc, identifiables par d'autres utilisateurs mal intentionnés. Cependant, la CIA aurait préféré profiter de ces faiblesses que d'en informer les développeurs d'objets connectés afin d'en améliorer la sécurité.

Cependant, ces failles ayant été rendues publiques, l'ensemble des fabricants et développeurs d'objets connectés ont déjà, ou sont en train d'œuvrer au colmatage de celles-ci.

A noter que la très grande majorité des malwares présentés par Wikileaks n'ont pas pour vocation un espionnage massif mais, vraiment des actions ciblées car nécessitant un accès physique à l'appareil en question. Tout un chacun ne peut donc pas être pris pour cible et espionné chez lui.

A retenir donc que les cybers menaces contre la France sont grandissantes, au même rythme que notre mode de vie se numérise et que notre dépendance au numérique s'amplifie.
Parallèlement, notre capacité de défense va crescendo aussi. Là où une menace apparait, une défense se met en place. C'est le propre de l'être humain de se défendre et de contre attaquer.

II -
Préfecture du Val-de-Marne
Cabinet du préfet

Créteil, le 2017

FICHE
A l'attention de
la Chambre de Commerce et d'Industrie
du Val-de-Marne

Objet : Cyber menaces : Quelles défenses pour la France

A l'heure actuelle, la cyber sécurité française est placé sous l'autorité du secrétaire général de la défense et de la sécurité nationale par le biais de l'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information qui oriente, assiste et coordonne les défenses.

Succédant en 2009 à la Direction Centrale de la Sécurité des Systèmes d'information, elle a vu, en 2013, ses prérogatives évoluer. D'un rôle de conseil, elle impose désormais la mise en place de mesures de sécurité adéquates aux administrations et OIV (Opérateurs d' Importance Vitale).
Elle est informée de tout incident pouvant avoir un impact sur l'intégrité des SI des administrations et OIV et, réalise régulièrement des audits afin de garder un niveau de sécurité le plus haut possible.
Elle coordonne également d'autres services de l'Etat afin d'identifier, endiguer et contrer de potentielles attaques.
L'an dernier, ce ne sont pas moins de 24000 attaques qui ont ainsi pu être bloquées en France.

A l'horizon 2019, il est également prévu au sein du ministère de la défense, la mise en place d'un commandement cyber défense. Il sera armé par 2600 militaires spécialisés et potentiellement soutenus par 4400 réservistes en cyber sécurité.

Par la création de cette entité, la France se placerait alors en tête des forces cyber européennes aux côtés des britanniques.

Le risque zéro n'existe pas mais, la France lutte au mieux pour s'en approcher.

2ème ÉPREUVE D'ADMISSIBILITÉ

Concours externe uniquement

Epreuve constituée d'une série de six à neuf questions à réponse courte portant, aux choix du candidat exprimé lors de l'inscription au concours, sur le programme de la spécialité choisie.

Les réponses sont rédigées, permettant ainsi de juger des qualités rédactionnelles du candidat.

Les questions posées peuvent porter sur l'exploitation, l'utilisation de matériels et/ou d'outils utilisés couramment dans la spécialité professionnelle et impliquer la réalisation de schémas ou de croquis partiels.

Spécialités proposées en 2017 :

- Gestion des systèmes d'information
- Génie électrotechnique
- Informatique et réseaux

(Durée : 3 heures ; coefficient 2)

Spécialité

GESTION DES SYSTEMES D'INFORMATION

Spécialité : Gestion des systèmes d'information

Vous veillerez à structurer suffisamment vos réponses.

1. Qu'est-ce qu'un protocole (enjeux, écueils, etc.) 2 points

2. Qu'est-ce que l'authentification (enjeu, différentes méthodes, niveaux, exemples de protocoles, etc.) 3 points

3. Base de données relationnelle 3 points

   Soient les entités *Employé* (IdEmployé, Nom) et Etablissement (IdEtablissement, Adresse)

   a. Règle de gestion : Un employé travaille dans un établissement et un seul. Donner la structure de ces deux entités sous forme de modèle logique des données (MLD).
   b. Modification de la règle de gestion : A présent, un employé peut travailler dans plusieurs établissements. Donner le MLD nécessaire pour répondre à ce nouveau besoin.
   c. Le MLD produit pour l'énoncé b) ne peut-il répondre à l'énoncé du a) ? Si oui pourquoi utiliser deux méthodes (avantages/inconvénients).

4. Les smartphones utilisent généralement diverses applications dédiées chacune à un besoin. Existe-t-il une autre alternative pour répondre à ce besoin ? 1 point

5. Qu'est-ce qu'un logiciel de gestion électronique de document (GED) ? (fonctionnalités, intérêt, exemples de solution, etc.) 2 points

6. La fonction n ! (factorielle n) est le produit des nombres entiers strictement positifs inférieurs ou égaux à n. Donner le code récursif de la fonction factorielle (n) (sous forme algorithmique ou langage de votre choix) [Ex. 4!=1 x 2 x 3 x 4 = 24 ou 4! =4 x 3 x 2 x 1 = 24] 3 points

7. Qu'est-ce que la méthode agile en développement logiciel ? (principes, objectifs, relation avec la maîtrise d'ouvrage, etc.) 3 points

8. Qu'est-ce qu'ITIL ? (domaine d'application, principes, plus-value, etc.) 3 points

SPECIALITE

COPIE AYANT OBTENU LA MEILLEURE NOTE À CETTE EPREUVE

MINISTÈRE DES ARMÉES

Session de 2017

CONCOURS

Pour l'accès à l'emploi de contrôleur spécialisé de classe normale
Épreuve : *de gestion des systèmes d'information*

Réservé à la notation

16,40 / 20

Question 1 :

- *Un protocole permet l'échange d'informations entre deux ou plusieurs parties qui peuvent être hétérogènes. A cette fin, il décrit entre elles un cadre et un langage communs (constitués de règles, conventions, structures de données etc.) qui assure l'échange et l'intégrité des données.*
- *Il existe de nombreux protocoles publics et normalisés qui réduisent l'effort de compréhension nécessaire à d'éventuels intrus mais permettent aussi l'analyse et la publication de leurs failles par, et toute la communauté d'utilisateurs. On peut citer les protocoles TCP pour l'élaboration d'une liaison de données ou SSH pour la connexion sécurisée à un terminal distant.*
- *Les protocoles « physiques » (qui impliquent du matériel) sont plus difficile à propager quand ils dictent le changement du matériel (on peut citer Ethernet ou les normes USB).*

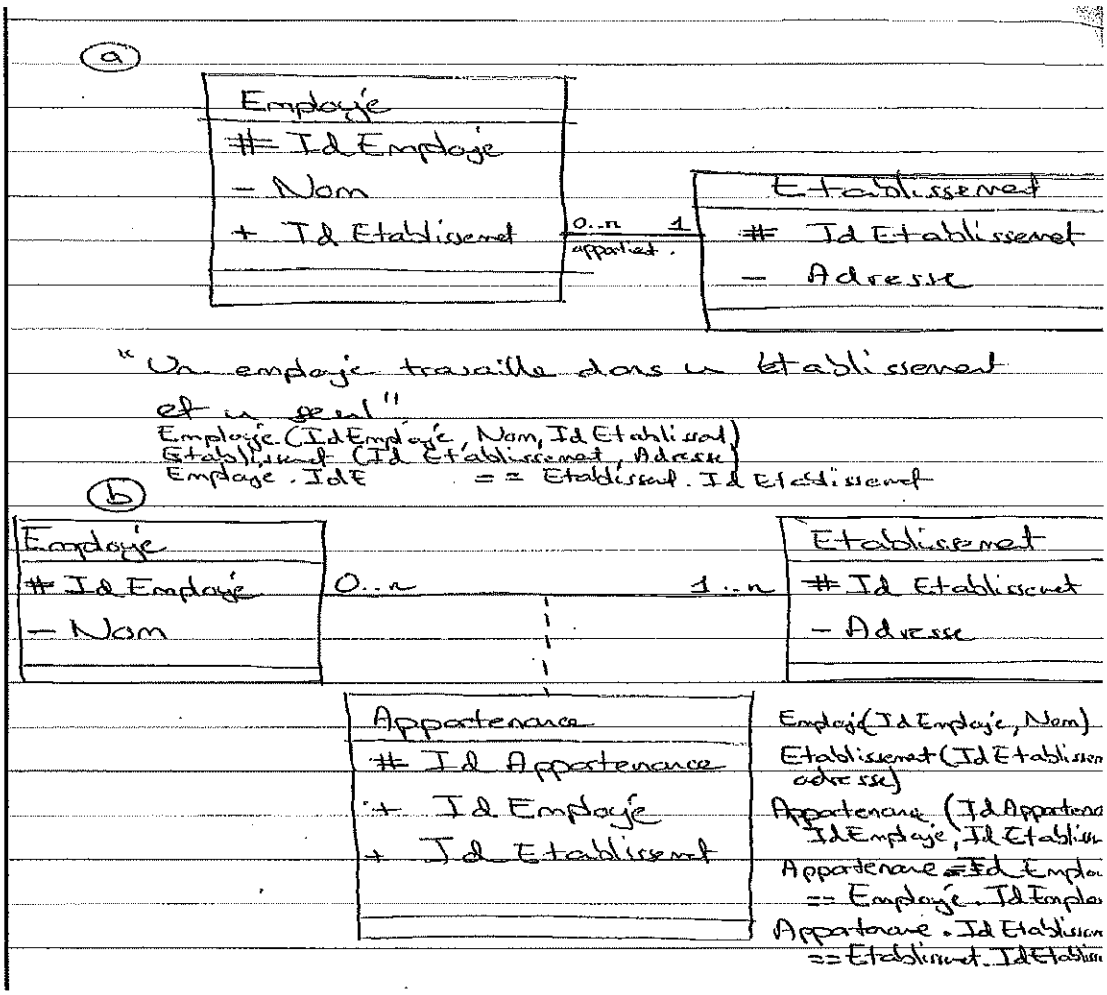
Question 2 :

L'authentification est un mécanisme qui permet de s'assurer de l'identité d'une personne (ou d'un système) quand elle accède à une ressource, comme un serveur, ou qu'on reçoit un message de sa part.

Une méthode simple d'authentification est l'établissement secret d'une paire identifiant/mot de passe sur un site Internet. Plusieurs niveaux de sécurité sont possibles comme le rajout d'un deuxième facteur (devoir transmettre un code reçu par un autre card comme les SMS).

Il est possible d'utiliser les certificats/le chiffrement, par l'inversion de l'utilisation des clés publiques et privées par exemple. Un protocole d'authentification du marché est Active Directory pour la connexion des utilisateurs Microsoft Windows.

Question 3 :



c- Le MLD produit par l'énoncé b) peut répondre à l'énoncé du a) en rajoutant une contrainte sur le nombre d'établissement par employé (=1).
La deuxième méthode permet une évolutivité plus facile de la base de données si le système charge.
Cependant elle va générer une table en plus ce qui coûtera en espace et en temps de calcul notamment lors des jointures. Cela peut devenir sensible sur de grosses quantités de données.

Question 4 :

Il existe plusieurs solutions pour répondre à un besoin sur un smartphone :

- *D'abord les applications dites natives qui intègre un programme conçu pour le système d'exploitation, qui stocke des données et peut exécuter des calculs en local et communiquer avec un serveur.*
- *Ensuite, on peut répondre au besoin sur un site Internet classique auquel l'utilisateur se connecte, via son navigateur. Un navigateur dédié peut être intégré à une mini-application pour rendre le processus transparent.*
- *Finalement, les applications dites hybrides qui combinent les deux approchent.*

Les applications natives ont l'avantage de pouvoir exécuter des calculs côté client, libérant de la bande-passante et du temps processeur côté serveur.

Les suites Internet ont l'avantage de permettre la mise à jour centralisée (côté serveur) et une meilleure portabilité si les normes du Web sont respectées. Les applications natives permettent l'utilisation hors-ligne mais doivent être développées pour chaque plate-forme, qui peut intervenir parfois (Google, Apple). Elles éparpillent aussi plus d'information (données, code).

Question 5 :

Un logiciel G.E.D permet de collecter, conserver, archiver et mettre à disposition les documents d'une entreprise ou d'une organisation. Il permet leur centralisation, contrôle et mise en valeur.

Question 6 :

Fonction Factorielle en pseudo - code =

```
Fonction Factorielle (n=entrée ; résultat : sortie)
{
Si (n=1)
Alors retourner (1\ ;
Sinon retourner (n × Factorielle (n - 1)) ;
FinSi
}
```

Question 7 :

Après avoir dressé le constat qu'un grand nombre de projets informatiques n'aboutissaient pas, on a créé la méthode agile avec l'ambition qu'elle fasse aboutir plus de projets qui satisfassent les clients.

Son principe est de découper le projet par cycles courts contenant chacun toutes les étapes classiques (conception, implémentation, test, recette).

A chaque début de cycle (ou « sprint ») le client ou son représentant (MOA, AMOM) est impliqué en exprimant ses besoins en commençant par les plus importants. Il est ainsi responsabilisé puisqu'il participe aussi à la recette de chaque cycle qui autorise le démarrage du cycle suivant. On ne développe ainsi pas plus que le besoin du client qui se voit assuré d'être couvert.

D'autres principes se greffent à la méthode agile comme la diminution de la documentation, le développement dirigé par les tests, etc... Des exemples de méthodes sont Scrum et Xtreme Programming.

Face aux difficultés à établir un budget pour les projets développés avec cette approche, ou face aux changements d'organisation et de gestion de projets majeurs nécessaires, les entreprises choisissent souvent des méthodes hybrides avec l'approche classique.

Question 8 :

ITIL est une démarche normalisée pour évaluer les processus dans une entreprise ou une organisation. Elle leur permet de vérifier et si besoin corriger ces méthodes de fonctionnement.

Elle permet d'obtenir une certification indépendante qui montre aux partenaires extérieurs (clients, investisseurs, etc...) qu'elles remplissent des critères de fonctionnement de qualité normalisés.

Spécialité

GENIE ELECTROTECHNIQUE

Spécialité : Génie électrotechnique

Question 1 : 6 points

Les Caractéristiques techniques d'un transformateur HTA/BT

Un : 20 kV/ 410 V
Puissance apparente : 1600 kVA
Ucc : 6%

		HTA	BT
Prises de réglage :	Prise 1	20,5 kV	
	Prise 2	20 kV	410 V
	Prise 3	19,5 kV	

a- Déterminer l'intensité nominale au primaire et au secondaire sur la prise 2 avec une tension de 20 kV au primaire :

b- SI on applique une tension de 20,8 kV sur la prise 1, quelle est la valeur de la tension BT ?

c- Que représente le Ucc et comment le mesure-t-on ?

d- Peut-on changer les prises de réglages du transformateur en charge ?

Question 2 : 6 points

Les impédances du transformateur

a- Un transformateur est-il plutôt résistif ou plutôt selfique ?

b- Quelle est l'impédance du transformateur vue de la basse tension ?

c- Si la résistance du transformateur est de l'ordre 3% de la réactance, déterminer la réactance et la résistance du transformateur pour une impédance de 7 Ω

Question 3 : 4 points

Les courants de défaut

a- Quelles sont les effets d'un courant de court-circuit sur le matériel et quel est le risque humain ?

b- Déterminer la puissance de court-circuit et le courant côté BT si en HTA, Il y a 250 MVA de puissance de court-circuit en tenant compte des caractéristiques du transformateur ci-dessus ?

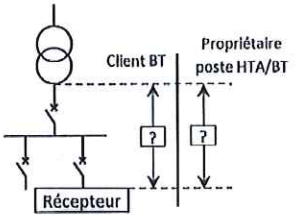
Question 4 : 5 points

Les chutes de tension

a- Pour un moteur qui consomme une puissance active de 350 kW avec un cos Ω de 0.8, déterminer la chute de tension en % au niveau des bornes BT du transformateur.

b- Quel remède à apporter pour minimiser la chute de tension ?

c- La norme NF 15-100 détermine les limites de la chute de tension à ne pas dépasser entre le point de raccordement BT et le récepteur, veuillez compléter le tableau ci-dessous :



	Eclairage	Autres usages (force motrice)
Alimenté par le réseau BT de distribution publique	%	%
Propriétaire de son poste HTA/BT	%	%

Valeur en pourcent

Question 5 : 3 points

La compensation de la puissance réactive

a- Sachant que le distributeur d'électricité applique une pénalité sur la puissance réactive lorsque la tangente φ dépasse 0,4, quelle est la quantité de condensateurs à installer pour éviter cette pénalité avec le moteur décrit ci-dessus ?

b- Quel est le moyen pour adapter les condensateurs en fonction du besoin ?

Question 6 : 6 points

Le variateur de vitesse

Nous avons décidé d'équiper le moteur asynchrone de 350 KW à 6 pôles d'un variateur de vitesse. Quels sont les avantages et inconvénients de ce système ?

a- Avantages :

b- Inconvénients :

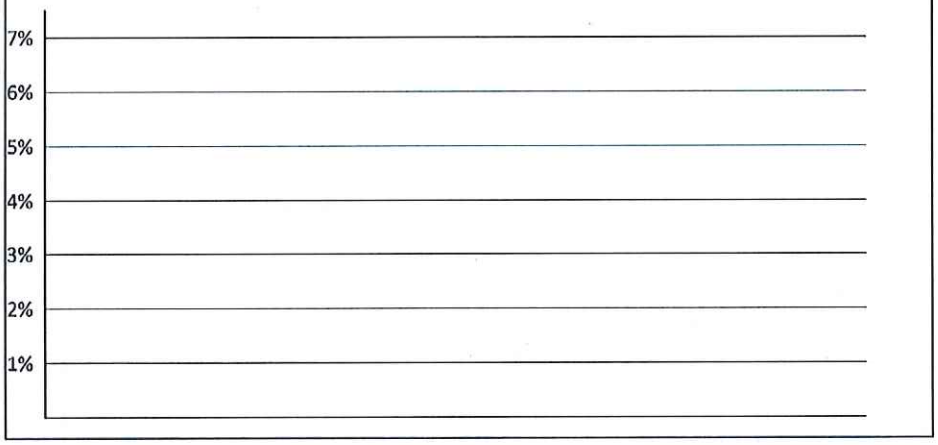
c- Calculer la fréquence en sortie du variateur pour que le moteur tourne à une vitesse de rotation de 200 tr/mn

Question 7 : 12 points

Les harmoniques:

a- Compléter le tableau ci-dessous, dessiner les spectres d'harmoniques correspondant, valeurs mesurées sur les courants de 75 A à 50 hz dans un réseau triphasé + Neutre BT:

	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11
taux	2%	5%	4%	6%	3%	7%	2%	5%	3%	4%
Hz										
courant										



b- Calculer le courant d'harmonique de rang 3 dans le neutre.

c- Par quels moyens peut-on se protéger des harmoniques ?

Indiquez plusleurs types

d- Dessiner un filtre passif série avec un condensateur de 10 µf et une réactance de 20,66 mH, calculer la fréquence de résonnance:

Question 8 : 10 points

Les régimes de neutre

a- Dessiner les différents régimes de neutre BT existants et expliciter l'intérêt :

Schéma IT :

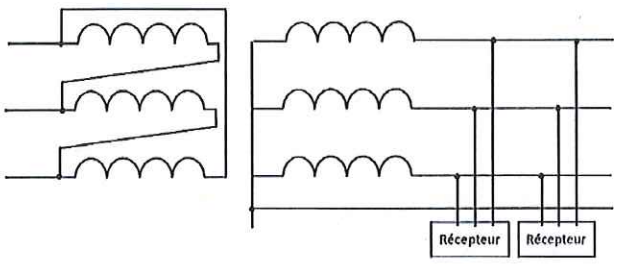


Schéma TT :

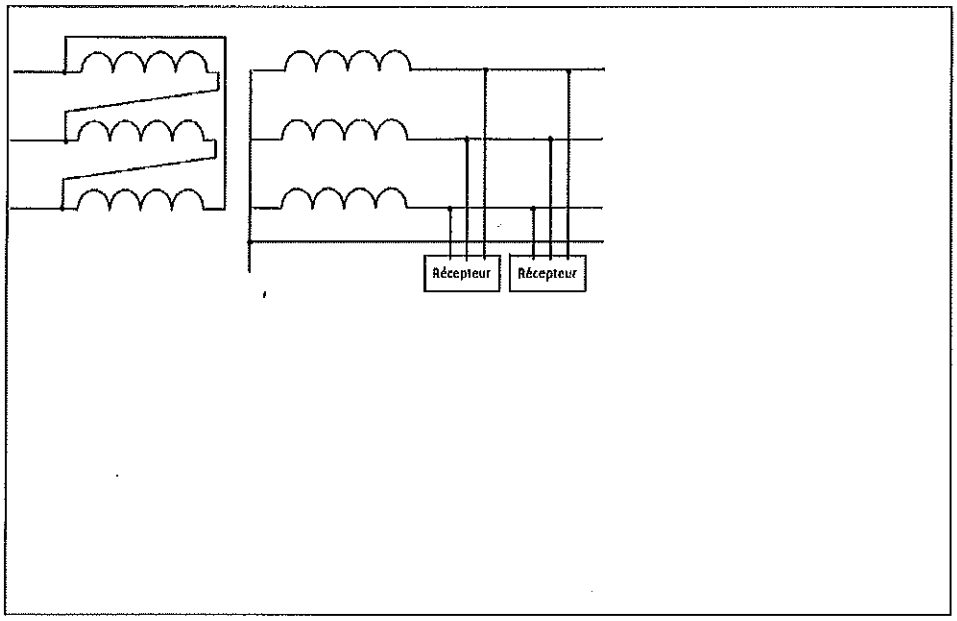


Schéma TNC :

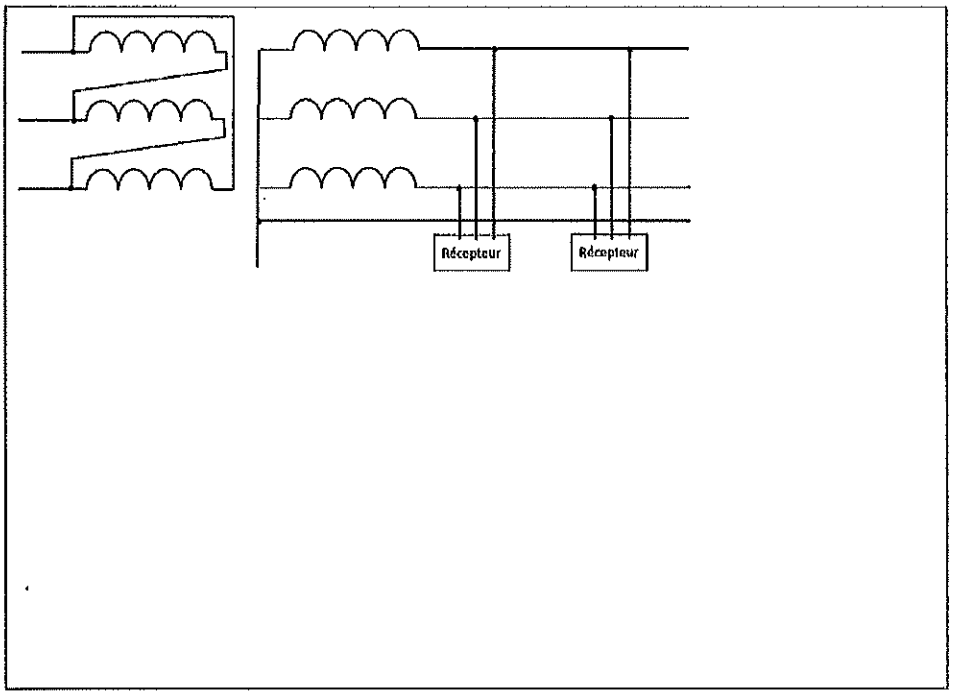
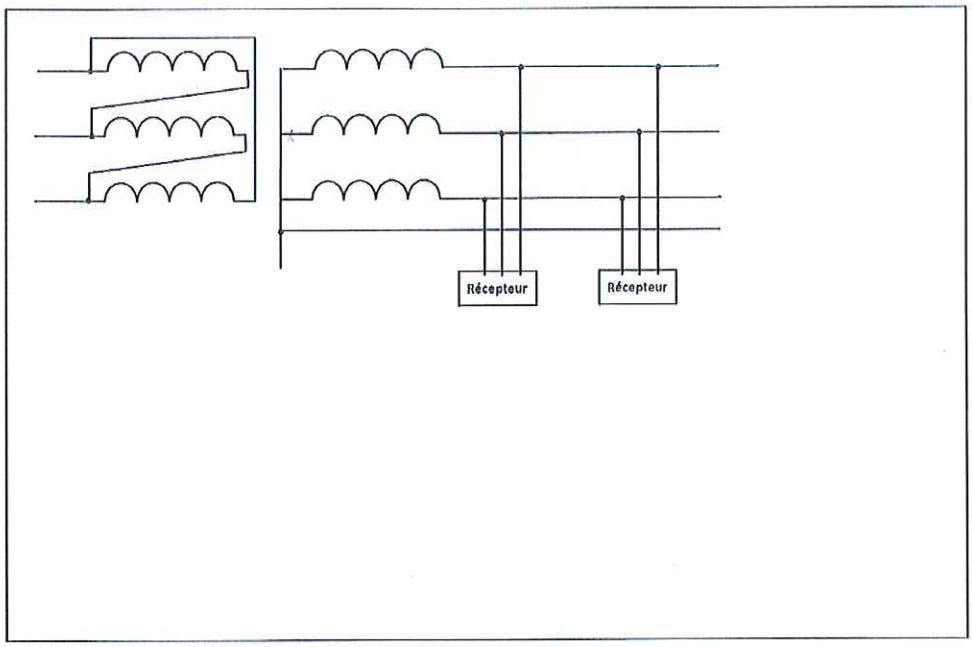


Schéma TNS :



Question 9 : 8 points

Les habilitations électriques

a- Quelle norme régit les habilitations ?

b- Rappeler les différents symboles d'habilitation

La première lettre :
B :
H :
Second caractère :
0 :
1 :
2 :
C :
R :
S :
P :
E :
Second indice :
V :
T :
N :
X :

c- Rappeler les 5 zones autour d'une partie nue sous tension qui concernent la HTA et la BT

Zone 0 :
Zone 1 :
Zone 2 :
Zone 3 :
Zone 4 :

SPECIALITE

COPIE AYANT OBTENU LA MEILLEURE NOTE À CETTE EPREUVE

MINISTÈRE DES ARMÉES

Session de 2017

CONCOURS

Pour l'accès à l'emploi de contrôleur spécialisé de classe normale
Épreuve : ***de génie électrotechnique***

Réservé à la notation

13,33/ 20

La correction du sujet a été réalisée avec les réponses de plusieurs copies pour vous apporter les solutions les mieux notées.

De ce fait, la note indiquée est celle qui aurait pu correspondre à la meilleure copie de cette spécialité.

Spécialité : Génie électrotechnique

Question 1 : 6 points

Les Caractéristiques techniques d'un transformateur HTA/BT

Un : 20 kV/ 410 V
Puissance apparente : 1600 kVA
Ucc : 6%

		HTA	BT
Prises de réglage :	Prise 1	20,5 kV	
	Prise 2	20 kV	410 V
	Prise 3	19,5 kV	

a- Déterminer l'intensité nominale au primaire et au secondaire sur la prise 2 avec une tension de 20 kV au primaire :

INTENSITÉ NOMINALE AU PRIMAIRE : $I_n = \frac{S}{\sqrt{3}\,U_n} = \frac{1600000}{20000\sqrt{3}} = 46{,}2\,A$

Intensité nominale au secondaire : $I_n = \frac{S}{U_n\sqrt{3}} = \frac{1600000}{410\sqrt{3}} = 2254\,A$

b- Si on applique une tension de 20,8 kV sur la prise 1, quelle est la valeur de la tension BT ?

On applique un produit en croix : 20,5 kV → 410 V ; 20,8 kV → 416 V
La valeur de la tension BT sera de 416 V.

c- Que représente le Ucc et comment le mesure-t-on ?

Ucc représente la tension U aux bornes du transformateur en Court-Circuit. Elle est exprimé en pourcentage de la Tension Nominale.

d- Peut-on changer les prises de réglages du transformateur en charge ?

Non. Il est impossible de changer les prises de réglages d'un transformateur en charge car il est nécessaire de décapoter celui-ci pour travailler dedans.

Question 2 : 6 points

Les impédances du transformateur

a- Un transformateur est-il plutôt résistif ou plutôt selfique ?

Un transformateur est plutôt selfique

b- Quelle est l'impédance du transformateur vue de la basse tension ?

c- Si la résistance du transformateur est de l'ordre 3% de la réactance, déterminer la réactance et la résistance du transformateur pour une impédance de 7 Ω

$Z = \sqrt{R^2 + X^2}$

$7 = \sqrt{\left(\frac{3 \times X}{100}\right)^2 + X^2}$

Question 3 : 4 points

Les courants de défaut

a- Quelles sont les effets d'un courant de court-circuit sur le matériel et quel est le risque humain ?

Les effets d'un court circuit sur le matériel sont de faire déjoncter la protection en amont du court circuit.
Il détériorera les cables avec le court circuit.
En théorie le risque humain est nul puisque le déjoncteur de protection aura déjoncté. Sinon l'humain risque de se faire électrisé.

b- Déterminer la puissance de court-circuit et le courant côté BT si en HTA, il y a 250 MVA de puissance de court-circuit en tenant compte des caractéristiques du transformateur ci-dessus ?

$I_{cc} = \frac{U_2}{\sqrt{3} \times Z_t} = \frac{410}{\sqrt{3} \times 7} = 33{,}8\ kA.$ Le courant de court-circuit côté BT sera de 33,8 kA.

$P_{cc_s} = U_{cc} \times I_{cc}$

$\frac{410 \times 6}{100} \times 33800$

$P_{cc_s} = 831{,}5\ kVA$ La puissance de court-circuit côté BT sera de 831,5 kVA.

Question 4 : 5 points

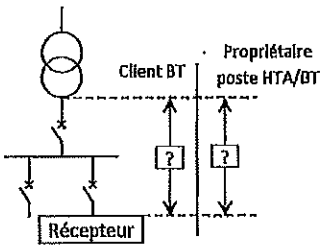
Les chutes de tension

a- Pour un moteur qui consomme une puissance active de 350 kW avec un cos Ω de 0.8, déterminer la chute de tension en % au niveau des bornes BT du transformateur.

b- Quel remède à apporter pour minimiser la chute de tension ?

Le remede possible pour minimiser la chute de tension est d'augmenter les sections des cables.

c- La norme NF 15-100 détermine les limites de la chute de tension à ne pas dépasser entre le point de raccordement BT et le récepteur, veuillez compléter le tableau ci-dessous :



	Eclairage	Autres usages (force motrice)
Alimenté par le réseau BT de distribution publique	7 %	5 %
Propriétaire de son poste HTA/BT	5 %	5 %

Valeur en pourcent

Question 5 : 3 points

La compensation de la puissance réactive

a- Sachant que le distributeur d'électricité applique une pénalité sur la puissance réactive lorsque la tangente φ dépasse 0,4, quelle est la quantité de condensateurs à installer pour éviter cette pénalité avec le moteur décrit ci-dessus ?

$Qc = Pa \times (Tan\,\varphi_{initial} - Tan\,\varphi_{final})$ (0,75 à été trouvé via le cosinus du moteur = tan(cos(0,8)) = 0,75)

$= 350\,000 \times (0,75 - 0,4)$

$Qc = 122\,500$ VAR

Il faudra installer une valeur de 122,5 kVAR de Condensateurs pour éviter les pénalités avec ce moteur.

b- Quel est le moyen pour adapter les condensateurs en fonction du besoin ?

Le meilleur moyen pour adapter les condensateurs en fonction du besoin à l'instant t est de choisir l'option à gradin. Lorsque l'on souhaite, nous pouvons ajouter ou retirer des valeurs de condensateurs en fonction du besoin fluctuant.
Des valeurs sont différentes selon les tailles et capacités installées.

Question 6 : 6 points

Le variateur de vitesse

Nous avons décidé d'équiper le moteur asynchrone de 350 KW à 6 pôles d'un variateur de vitesse.
Quels sont les avantages et inconvénients de ce système ?

a- Avantages :

Les avantages à installer un variateur de vitesse à ce moteur sont :
- les démarrages du moteur seront progressif, donc pas d'appel de courant au démarrage.
- Contrôle Intégrale du couple moteur via la fréquence imposée.

b- Inconvénients :

Les inconvenients à vouloir installer un variateur de vitesse à ce moteur sont les suivants :

- La production devra être arrêter pour le montage du Variateur
- le variateur de vitesse va produire des Harmoniques.

c- Calculer la fréquence en sortie du variateur pour que le moteur tourne à une vitesse de rotation de 200 tr/mn

$f = p \cdot n$

f : fréquence ; p : nombre de paire de pôles ; n : vitesse en tr/s

$f = p \cdot n$

$f = 3 \times \frac{200}{60}$

$f = 10$ Hz

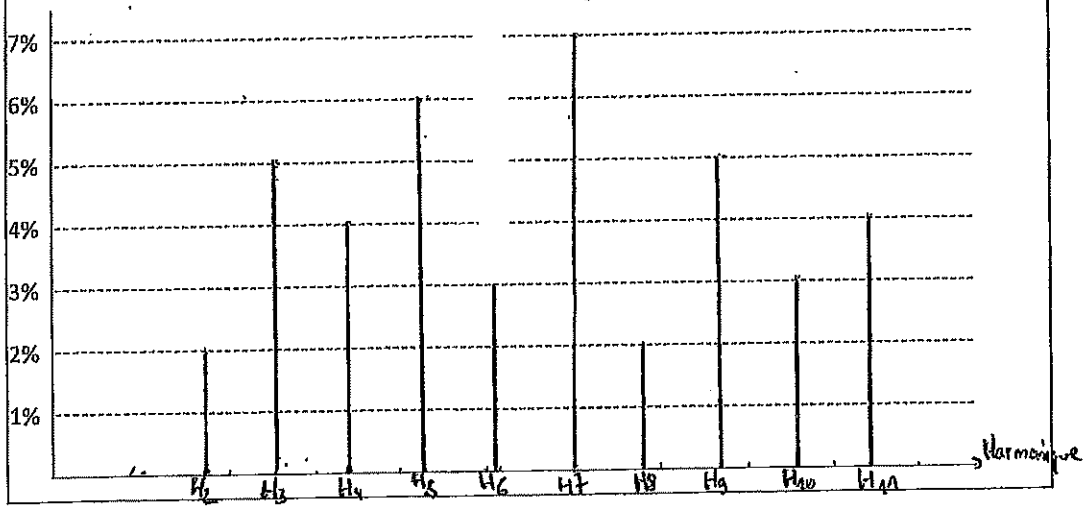
La fréquence de sortie du variateur devra être de 10 Hz pour que le moteur atteigne une vitesse de rotation de 200 tr/minute.

Question 7 : 12 points

Les harmoniques:

a- Compléter le tableau ci-dessous, dessiner les spectres d'harmoniques correspondant, valeurs mesurées sur les courants de 75 A à 50 hz dans un réseau triphasé + Neutre BT:

	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11
taux	2%	5%	4%	6%	3%	7%	2%	5%	3%	4%
Hz	1	2,5	2	3	1,5	3,5	1	2,5	1,5	2
courant	1,5	3,75	3	4,5	2,25	5,25	1,5	3,75	2,25	3



b- Calculer le courant d'harmonique de rang 3 dans le neutre.

Le courant d'harmonique de rang 3 circulant dans le neutre est:
$I_N = I_1 + I_2 + I_3 = 3,75 \times 3 = 11,25\,A$

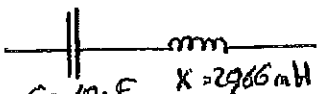
c- Par quels moyens peut-on se protéger des harmoniques ?

Indiquez plusieurs types

On peut se protéger des harmoniques en installant des compensateurs d'harmonique de type Actif ou passif. (type Sinewaves (actif) ou FAH (passif) de chez Schneider Electric)
Ou en installant sur le réseau des Condensateurs.
On peut également installer à plusieurs point du réseau des transformateurs d'isolement, mais cette solution reste cher et encombrante.

d- Dessiner un filtre passif série avec un condensateur de 10 µf et une réactance de 20,66 mH, calculer la fréquence de résonance:

Représentation d'un filtre passif série avec un condensateur et une réactance



Calcul de la fréquence de résonance :

$f = \sqrt{\frac{1}{(2\pi)^2 LC}} = \sqrt{\frac{1}{(2\pi)^2 \times 20{,}66.10^{-3} \times 10.10^{-6}}}$

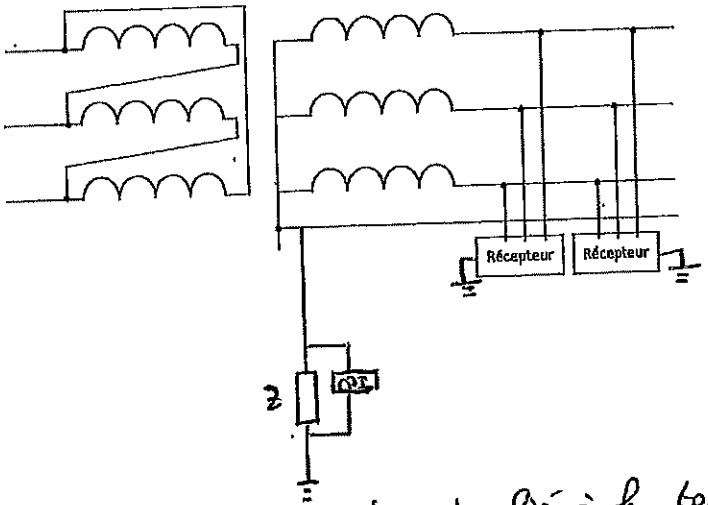
$f = 350{,}2\,Hz$

Question 8 : 10 points

Les régimes de neutre

a- Dessiner les différents régimes de neutre BT existants et expliciter l'intérêt :

Schéma IT :



I signifie que le neutre est relié à la terre avec une impédance. Cette impédance est contrôlée par un "Contrôleur permanent d'isolement (CPI)
T signifie que les masses des récepteurs sont reliés à terre.
Si un défaut survient, le disjoncteur ne s'arrête et le CPI prévient d'un défaut. Il y aura déclenchement au 2ème défaut.

Schéma TT :

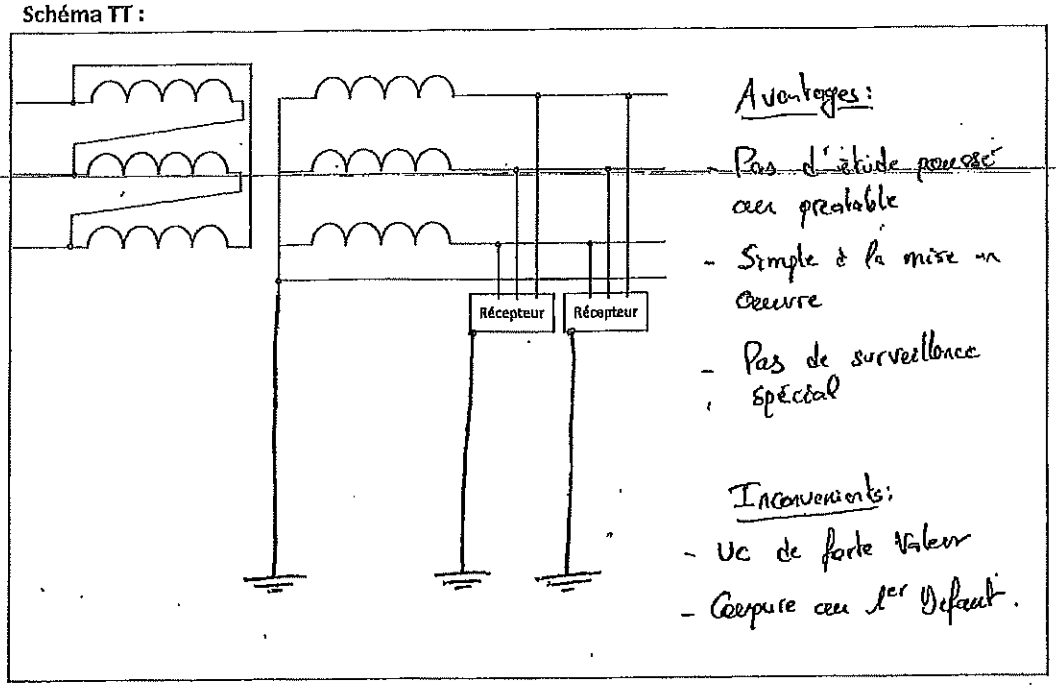


Schéma TNC :

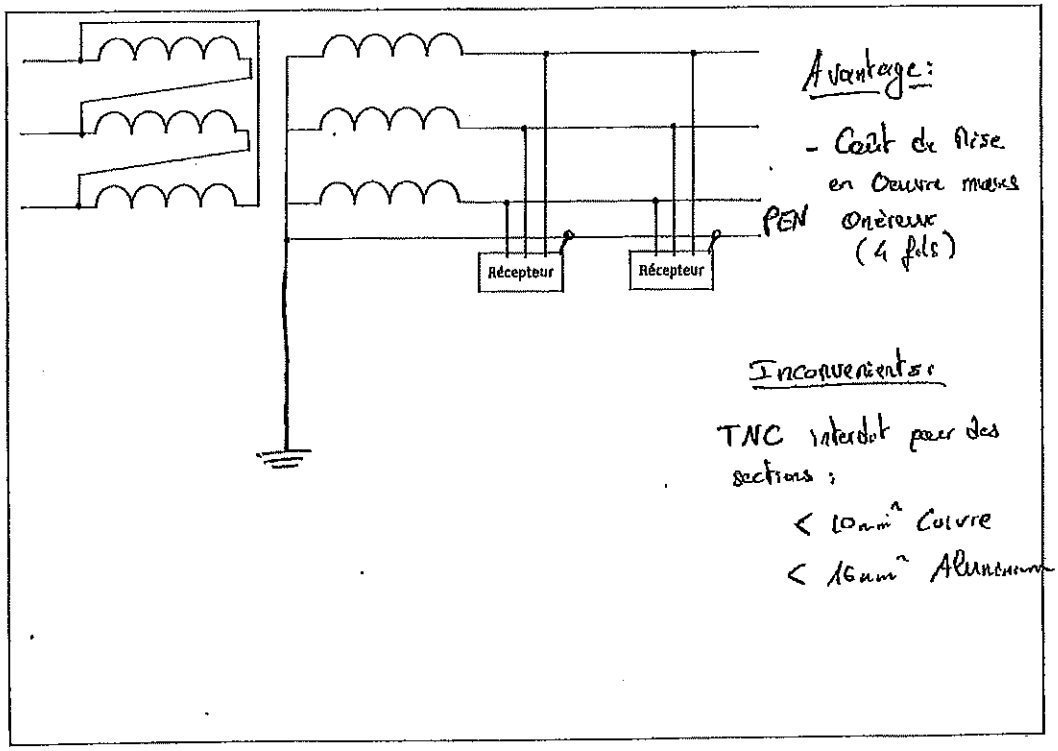
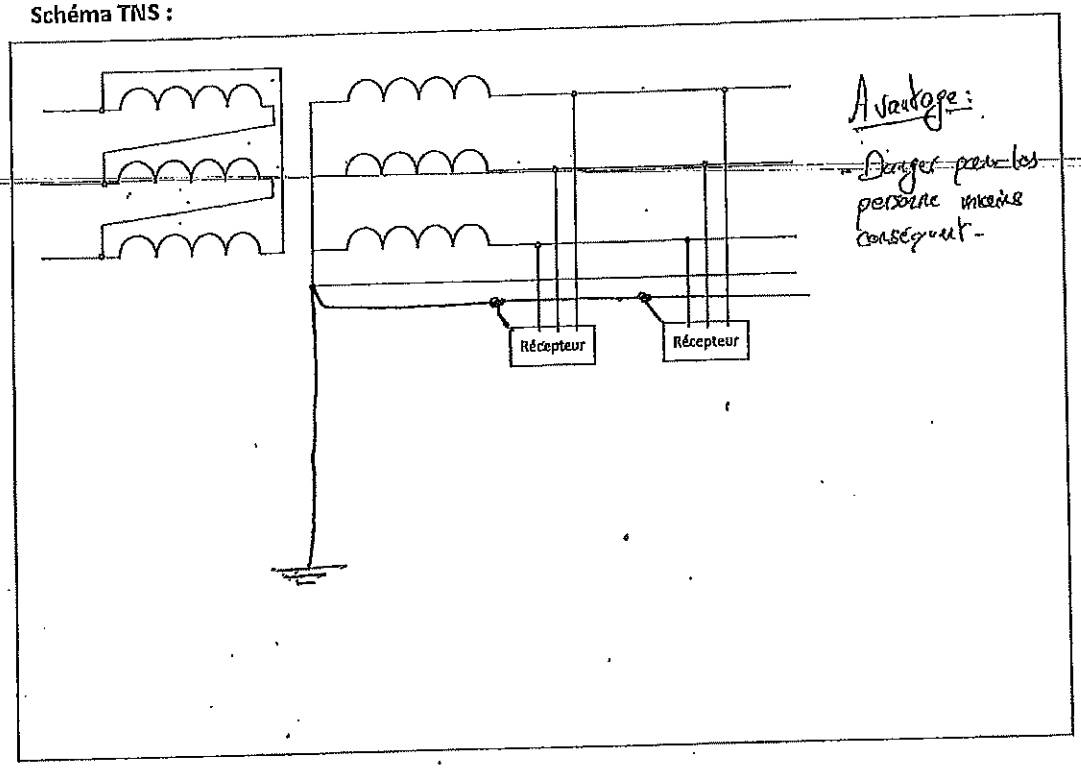


Schéma TNS :



Question 9 : 8 points

Les habilitations électriques

a- Quelle norme régit les habilitations ?

La norme qui régit les habilitations est UTE-18-510

b- Rappeler les différents symboles d'habilitation

La première lettre :
B : Basse Tension
H : Haute Tension
~~*Second caractère :*~~
0 : Non Electricien
1 : Exécutant Electricien
2 : Electricien Confirmé
C : Chargé de Consignation
R : Chargé de Travaux
S :
P : Photovoltaïque
E : Mesures et Essais
Second Indice :
V : Concerne le Voisinage (Travaux/opération au voisinage)
T :
N :
X : Zone Atex

c- Rappeler les 5 zones autour d'une partie nue sous tension qui concernent la HTA et la BT

Zone 0 :	En HTA = 1 m	en BT = 5 cm
Zone 1 :	En HTA = 1,5 m	en BT = 30 cm
Zone 2 :	En HTA = 3 m	en BT = 1 m
Zone 3 :	en HTA = 5 m	en BT =
Zone 4 :	en HTA = > 7 m	en BT =

Spécialité

INFORMATIQUE ET RESEAUX

Concours externe de contrôleur spécialisé de classe normale session 2017

Spécialité : Informatique et réseaux

- Examen sur 60 points - note ramenée sur 20.

Question 1 : (8 points)

a- Quelle est la différence entre un câble UTP droit et croisé ? Comment peut-on les différencier ?
b- Citer un exemple d'utilisation d'un câble UTP croisé.
c- Qu'est-ce qu'une épissure ?
d- Qu'est-ce qu'un test de réflectométrie ?
e- Quels sont les deux types de fibre optique ?
f- Donner trois types de connecteurs optiques standards.
g- Donner trois types de polissage des extrémités de connecteur optique.

Question 2 : (6 points)

Traduire les acronymes ci-dessous et y associer une définition :

a- LAN
b- WAN
c- SAN
d- DMZ
e- VPN
f- VLAN

Question 3 : (6 points)

a- Qu'est-ce qu'une adresse MAC ?
b- Décrire chronologiquement les actions qui se déroulent après avoir lancé la commande « ping www.google.fr » depuis une station correctement configurée et connectée sur un réseau local d'entreprise.
c- Une boucle physique réseau :
   - Quelle en est la définition ?
   - Quels en sont les symptômes ?
   - Pouvez-vous expliquer le phénomène physique ?
   - Quel mécanisme peut remédier à la problématique associée ?

Question 4 : (6 points)

a- Quels sont les trois paramètres constituant la configuration IP de base de la carte réseau d'un poste de travail ?
b- Expliquer la différence entre une adresse IP publique et une adresse IP privée.
c- Pourquoi les deux types d'adresses existent ?

d- Définir les plages d'adresses IP privées définies par la RFC1918.
e- Citer deux mécanismes permettant à une station munie d'une adresse IP privée d'accéder à Internet ?
f- Citer quatre informations contenues dans un en-tête IP ?

Question 5 : (12 points)

a- Soit l'adresse 172.16.9.10/28. Quel est le masque réseau associé, en représentation binaire et décimale ?
b- Vous disposez de l'adresse réseau 200.35.3.0/24. Il vous est demandé de découper ce réseau en plusieurs sous-réseaux pour que chacun puisse héberger 20 stations.
   - Combien de bits sont nécessaires sur la partie hôte ?
   - Combien d'adresses hôtes sont alors disponibles dans chaque sous-réseau ?
   - Détailler le second sous-réseau : réseau/masque, adresse de réseau, plage d'adresse hôte, adresse de diffusion.

Question 6 : (8 points)

a- Recopier sur votre copie le tableau ci-dessous et compléter les cases vides en associant pour chaque nom de protocole le ou les ports standards avec lesquels il fonctionne.

Protocole	N° de port
	69
NTP	
	20/21
	22
HTTPS	
	53
	25

b- Quelles sont les principales informations contenues dans un en-tête TCP ?

Question 7 : (4 points)

a- Proposer le schéma d'une infrastructure DMZ. Vous utiliserez exclusivement les éléments figurant dans la liste indiquée ci-dessous :
   - LAN
   - Internet
   - Pare-feu Interne
   - Pare-feu Externe
   - Proxy http
   - Relais SMTP
   - Serveur de messagerie Interne
   - Utilisateur
   - Serveur web Internet
b- Modéliser sur le schéma le cheminement d'un flux http d'un client interne vers le serveur web Internet.

SPECIALITE

COPIE AYANT OBTENU LA MEILLEURE NOTE À CETTE EPREUVE

MINISTÈRE DES ARMÉES

Session de 2017

CONCOURS

Pour l'accès à l'emploi de contrôleur spécialisé de classe normale
Épreuve : *informatique et réseaux*

Réservé à la notation

17,50/ 20

Question 1

a) *La différence entre les deux types de câbles droit et croisé est le sertissage des câbles, les fils ne seront pas positionnés au même endroit sur les deux extrémités du câble croisé.*
Le plus simple pour les différencier, est de prendre un câble, de mettre les deux extrémités côte à côte et d'identifier les brins, si l'ordre des couleurs est le même les convecteurs, c'est un câble droit sinon c'est un câble croisé.

b) *Un câble UTP croisé, sera principalement utilisé pour raccorder un ordinateur à un routeur.*

c) *Une épissure est le terme employé pour identifier chaque brin d'un toron de câble, par exemple pour un accès opérateur.*

d) *Un test de réflectométrie est le processus utilisé pour qualifier une fibre optique de bout en bout.*

e) *Les deux types de fiche sont monomode et multimode.*

f) *LC/LC, LC/SC, SC/APC, sont trois types de connecteur optique disponibles.*

g) *Les trois types de polissage sont en biseau, circulaire et rectangulaire.*

Question 2

a) *LAN / Local Area Network, terme employé pour définir le réseau local d'entreprise.*

b) *WAN : World Area Network, défini le réseau d'entreprise à travers les accès opérateurs.*

c) *SAN : Storage Area Network, est le stockage système hébergé sur le réseau et non sur le disque dur local. On peut également trouver une autre définition et acronyme associé, qui est Subject Alternative Name, qui est un élément contenu dans un certificat électronique.*

d) *DMZ : Demilitarized Zone, est une zone hors réseau utilisateur ou sont principalement hébergés les serveurs de l'entreprise.*

e) *VPN : Virtual Private Network, est un moyen pour permettre à un utilisateur d'accéder au service d'information de son entreprise. Le cas le plus courant est le télétravail.*

f) *VLAN : Virtual Local Area Network, est un LAN logique, un seul équipement physique peut supporter et gérer plusieurs LAN. Exemple, deux réseaux bien distincts, Service informatique, Service vente.*

Question 3

a) *Une adresse MAC est l'adresse d'une prise réseau « active » par exemple, celle d'un ordinateur, celle d'un commutateur…*

b) *Lors de la saisie de la commande « ping www.google.com » la chronologie est la suivante :*
Requête ARP sous le serveur DNS
Réponse avec l'adresse IP du serveur DNS
Requête DNS sur www.google.com
Réponse DNS avec l'adresse IP associée
Requête ARP vers la passerelle par défaut
Réponse ARP avec l'adresse IP de la passerelle
Requête ICMP vers l'adresse IP retournée par le serveur DNS

Traversé des pockets jusqu'à l'hôte
Réponse ICMP du serveur « www.google.com

Question 4

a) *Les trois paramètres principaux d'une carte réseau sont : l'adresse IP, le masque de sous réseau et la passerelle par défaut.*

b) *Les adresses IP publiques sont rentables sur Internet. Seules ces adresses la sont connues d'Internet. Les adresses IP privées sont utilisées sur le réseau local d'entreprise uniquement.*

c) *Les deux types d'adresses existent car il y a une pénurie d'adresse IP publique. De plus cela permet également de protéger son réseau local d'Internet.*

d) *10.0.0.0/8*
172.16.0.0/12
192.168.0.0/16
Ce sont les trois plages d'adresses IP privées.

e) *Pour accéder à Internet, il y a les mécanismes NAT et le tunnel VPN vers un opérateur raccordé à Internet.*

f) *Dans une en tête IP on peut trouver l'adresse IP source, l'adresse IP de destination, le champ TOS et le plug du protocole suivant (6 pour TCP et 17 pour UDP).*

Question 5

a) *Pour l'adresse 172.16.9.10/28 le masque associé est :*
Binaire : 11111111.11111111.11111111.1111.0000
Décimal : 255.255.255.240

b) *Soit le réseau 200.35.3.0/24*
1- *Pour avoir 20 stations par sous réseaux, il faut 5 bits dans la partie hôte, $2^5 = 32$.*

2- *Il y a 2^5-2 hôtes utilisables, soit 32 -2 = 30 hôtes utilisables.*

3- Le second réseau est 200.35.3.32/27
@Réseau : 200.35.3.32
@ Diffusion : 200.35.3.63
Plage d'@ : 200.35.3.33
: 200.35.3.62

Question 6

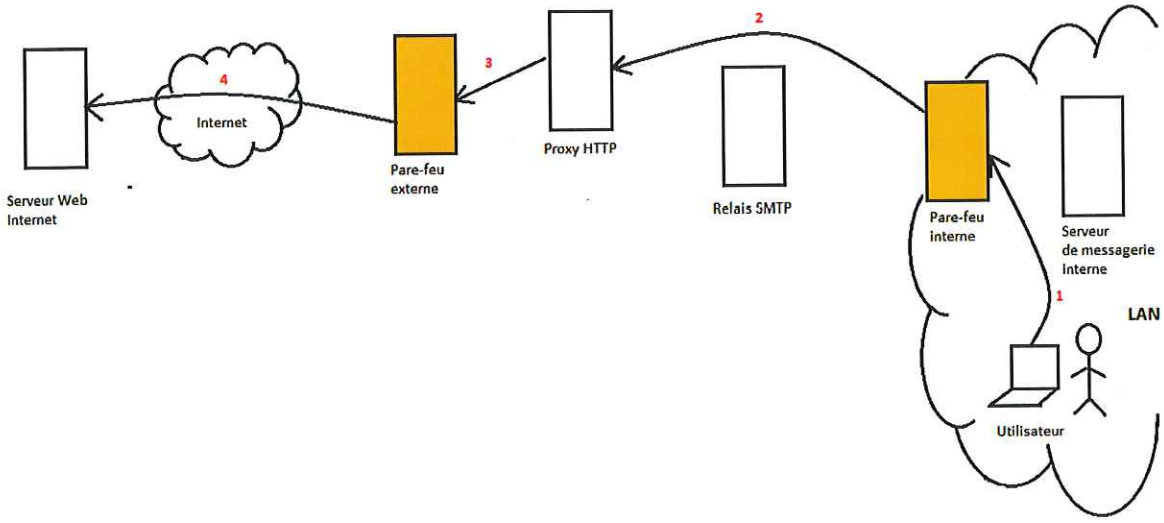
a)

Protocole	N° de port
TFTP	69
NTP	123
FTP	20/21
SSH	22
HTTPS	443
DNS	53
SMTP	25

b) Les principales informations d'une en tête TCP sont adresse IP source, adresse IP destination, port source, port destination.

Question 7

a) Schéma



1- Requête sur le serveur web

2- Contrôle de l'autorisation sur le pare-feu interne + envoi au proxy http

3- Contrôle de l'autorisation sur le pare-feu externe

4- Envoi des pockets à destination du serveur web.

b) Le rôle d'un serveur proxy, est de masquer l'identité des clients en modifiant l'adresse IP source. L'émetteur n'est plus l'utilisateur mais le serveur proxy.

c) Le pare-feu a pour fonctions principales d'autoriser ou non les utilisateurs à accéder à différents services, par exemple web, messagerie, transfert de fichiers... mais également de faire de l'inspection de pockets afin de vérifier que ces derniers sont conformes.

Question 8

a) Sans espace, cela renvoi une erreur ls-la /etc liste le contenu du dossier /etc sous forme de liste incluant les fichiers cachés.

b) Sans espace, cela renvoi une erreur néanmoins il manque le fichier à la suite du-h.

c) Sans espace, cela renvoi une erreur mais ps-aef > fichier.txt renvoi le résultat de la commande ps-aef dans le fichier « fichier.txt ».

d) Le fichier.txt bis crée un lien symbolique, « un raccourci » de fichier.txt nommé « bis ».

e) Chmod g-w, o-w permet de retirer le droit d'écriture à tout le monde excepté au propriétaire. En revanche, il manque le nom du fichier sur lequel ces changements doivent être appliqués.

Question 9

a) Un certificat électronique est un conteneur dans lequel plusieurs informations propres au détenteur sont stockées. Dans le cas d'un échange chiffré, il permet de s'assurer de l'identité de l'interlocuteur.

b) Voici 4 champs de base contenu dans un certificat
Common Name (identité)
Issuer (signataire)
Date de validité (not before, note after)
Subject Alternative Name (alias de Common Name)

c) *Une JGC est un tiers de confiance mais également le plus au niveau de la chaîne de certification. Elle permet notamment de signer les certificats clients, elle stocke toutes les clés publiques des certificats signés, cela permet de vérifier l'authenticité des clés publiques présentées lors d'un échange à base de certificat.*

ÉPREUVES D'ADMISSION

(COMMUNES AUX 2 CONCOURS)

ÉPREUVE D'ADMISSION

Une épreuve orale consistant en un entretien avec le jury destiné à apprécier les qualités personnelles du candidat, ses motivations, son potentiel, son comportement face à une situation concrète, le cas échéant sous forme de mise en situation.

Pour conduire cet entretien, le jury dispose d'un dossier constitué par le candidat :

a. Le candidat au concours externe fournit une fiche individuelle de renseignement, d'un curriculum vitae et d'une lettre de motivation.

b. Le candidat au concours interne établit un dossier de reconnaissance des acquis de son expérience professionnelle.

(durée : 25 minutes, dont 10 minntes au plus d'exposé ; coefficient 4)