Informaticien

Concours externe 2017

MEILLEURES COPIES

Spécialité "Informaticien de production"

ASSEMBLÉE NATIONALE
Service des Ressources humaines

ASSEMBLÉE NATIONALE

SOMMAIRE

ASSEMBLÉE NATIONALE

000055

NOTE : 14 /20

Concours : INFORMATICIEN

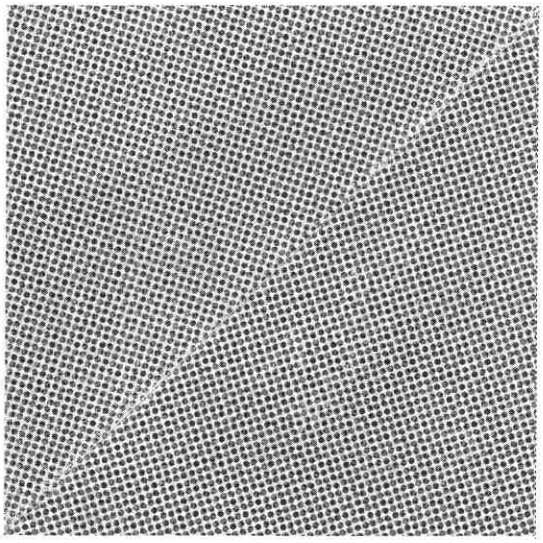
Épreuve : Questionnaire commun

Copie n° : 1 / 2

Question 1

Un gestionnaire de version est l'outil collaboratif qui permet de gérer les sources (fichiers) d'un projet. Tout d'abord, présent dans les environnements de développement, il a aussi séduit les exploitants des environnements de production.
Les services rendus sont les suivants:

- gestion des versions: toutes modifications d'un fichier entraîne la création d'une nouvelle version du document qui est datée et numérotée (numérotation généralement incrémentale).
- mécanisme de publication: l'ensemble des documents peuvent être accessibles via le réseau en utilisant un protocole propriétaire ou via les protocoles web standards comme http(s) ou Ftp(s). La publication a deux objectifs:
  - utiliser les fichiers sources dans le cadre de l'exploitation (déploiement d'un programme, mise à jour, ...)
  - contribuer aux développements du projet
- mise à jour d'un fichier: un mécanisme d'envoie d'une nouvelle



version d'un document permet la mise à jour et déclenche le dispositif de gestion de versions. Il doit être capable de gérer les conflits et de retourner aux contributeurs des messages explicites.

gestionnaire de branches : un projet peut prendre plusieurs orientations pour des motivations diverses comme des niveaux de stabilité différents (stable ou dev) ou encore des choix technologiques différents (utilisation librairie c++ ou python). Le gestionnaire de branches permet au sein du même projet de gérer ses différentes orientations

Un gestionnaire de version couremment utilisé est git
Il dispose de toutes les fonctions de base (enoncée ci-dessus) et est très présent dans les environements de « dev » et de « production ».

Le travail en equipe nécessite tout d'abord de s'organiser autour de l'outil. Il faut decider: Comment sera géré le dépôt? Comment seront gérés les branches? Est-ce que tous les contributeurs ont un rôle égal? Quelles sont les règles de MAJ? Ensuite, il faut créer le dépôt et gérer les modes d'accès en fonction du mode de publication (Intranet ou Internet)

La creation du dépôt aura bien evidemment requis en amont l'étude de l'infrastructure d'hébergement (serveurs existants ou nouvelles plateformes).
Les contributeurs devront finalement installer (ou faire installer) un client local qui permettra les mises à jour tout en respectant les règles établies lors de la première phase.

Question 2

Les 5 operations de bases des bases de données relationnelles sont

- la requête (ou query): Elle permet de sélectionner une liste d'occurences pour être afficher ou faire l'objet d'une autre opération (insertion, mise à jour, ...) Elle est associée à une fonction appelée la jointure qui permet d'effectuer des requêtes sur plusieurs tables en realisant des operations de comparaisons logiques ou mathématiques entre attributs de plusieurs tables. On peut ainsi realiser des requêtes de type :
  - produit cartésien
  - union
  - intersection
  - division
  - sous requête

En SQL, ce sont les mots clés suivants qui sont utilisés

- SELECT ... FROM ... WHERE ... (JOIN ...)
- UNION / EXIST / IN / ...

- la mise à jour (ou update) Elle permet la mise à jour d'un ou plusieurs attributs d'une table. Un filtre peut être appliqué pour sélectionner une liste d'occurences
  En SQL, c'est la notation suivante qui est généralement utilisé :
  - UPDATE ... SET ... WHERE ...
- l'insertion (ou insert) Elle permet d'insérer une occurence dans une table. Associer à la clause SELECT, elle peut insérer une liste d'occurences.
  En SQL, c'est la notation suivante qui est généralement utilisée :
  - INSERT ... INTO ... (SELECT ...)
- la suppression (ou delete) Elle permet de supprimer une ou plusieurs occurences en fonction d'un filtre au sein d'une même table.
  En SQL, c'est la notation suivante qui est utilisée :
  - DELETE ... WHERE ...
- la création et la destruction qui permettent de créer et détruire une table. Pour la création, la syntaxe dépend du SGBD.
  En SQL : CREATE table ... et DROP table ...

ASSEMBLÉE NATIONALE

000055

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : Questionnaire commun

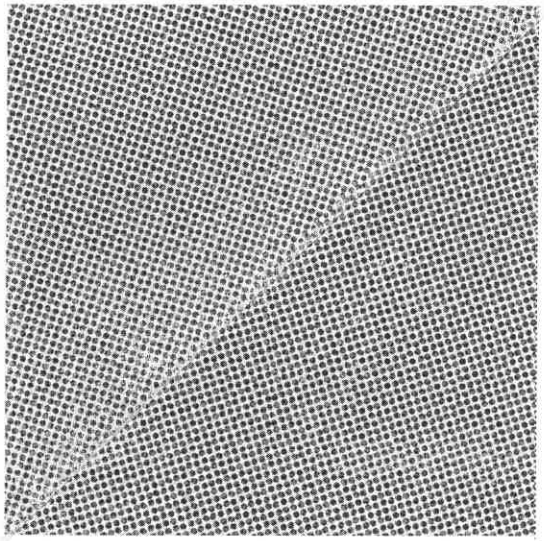
Copie n° : 2 / 2

le langage principal reposant sur le modèle relationnel est le SQL.

Question 3

L'analyse des risques est nécessaire avant la conception d'un projet car elle permet :

- identifier la faisabilité d'un projet : Il peut en effet s'avérer qu'un projet puisse s'avérer non viable pour des raisons de coûts, de ressources ou de temps.
- clarifier les besoins : Si ce n'est pas son objectif principal, cette étape permet aux différents acteurs d'exprimer clairement leurs besoins.
- définir l'environnement : Il faut s'assurer que l'environnement est en adéquation avec le projet. Si le SI n'est pas adapté, il faut étudier le coût de l'adaptation. Ainsi, on ne construit pas un "datacenter" en zone inondable.



Question 4

Le rôle du service DNS est principalement le service de noms. C'est à dire la capacité de traduire un nom en une adresse IP (v4 et v6)
Basiquement, c'est un mode client-serveur basé sur le protocole du même nom "DNS" dont le port d'ecoute du serveur est le 53. Il utilise deux principaux mécanismes :

- itératif : on demande à celui qui requête d'aller interroger un autre serveur
- récursif : le serveur qui reçoit la requête va rechercher la réponse chez un autre serveur

Le problème du protocole DNS, c'est que les requêtes et réponses ne sont pas nativement chiffrés. Pour résoudre ce manque de sécurité, deux mécanismes ont été crées :

- client - serveur : utilisation du TLS
- serveur - serveur : DNSSEC

Les enregistrements les plus courants sont :

- A traduction d'un nom en une adresse
- CNAME lien d'un nom vers un autre nom
- PTR traduction d'une adresse vers un nom

- TXT champs texte pour utilisation diverses comme le SPF
- MX indique les serveurs de messagerie
- NS indique les serveurs DNS
- SOA enregistrement qui décrit la zone

Question 6

La commande TOP est constituée de deux zones :

- En haut des informations globales sur le système :
  - les tâches en cours et le nombre de processus par état
  - le taux d'utilisation des CPU
  - la taille et le pourcentage d'utilisation de la mémoire vive
  - la taille et le pourcentage d'utilisation des zones SWAP
- En bas des informations par processus classés par utilisation décroissante des CPUs :
  - id du processus
  - utilisateur qui a lancé le processus
  - priorité du processus
  - ...
  - pourcentage d'utilisation du CPU de la mémoire

- la commande (le programme) lié au processus

Dans notre cas, on remarque que le serveur est chargé car le SWAP est fortement utilisé 3964844/4194300 KiB. Aussi les deux processeurs sont sollicités. Il reste de la mémoire vive mais on imagine qu'elle a été libérée par les mécanismes de SWAP. Le processus mysqld occupe 41,5% des processeurs.
Je proposerai donc de diviser les fonctions de LAMP:
- créer un serveur pour héberger mysql
- créer un serveur pour Apache et PHP

Question 5

La méthode en V est basée sur la réalisation d'étapes successives: définition du besoin, etude de l'existant, modélisation et spécifications, conception, tests (recette, préproduction et production), intégration. Le développeur travaille hors de la production. Les méthodes agiles sont basées sur des cycles itératifs et un rapprochement des equipes de dev et de production. Il n'y a pas un livrable comme dans le cycle en V mais une successions de livraisons.
Le cycle en V est donc plus adapté au gros projet car il est très organisé alors que le developpement Agile est adapté au petit projet où il faut plus d'adaptabilité.

ASSEMBLÉE NATIONALE

000212

NOTE : 18,5 /20

Concours : INFORMATICIEN

Épreuve : PRODUCTION

Copie n° : 1 / 7

1ère partie

1) L'étude du niveau de sécurité du SI va comporter deux principales étapes qui correspondent aux documents en annexe :

- Etude de l'architecture réseau et sécurité (annexe 1)
- Analyse des systèmes et des vulnérabilités (annexe 2)

L'étude de l'architecture réseau et de sécurité nous montre que l'infrastructure de C-NA est très peu sécurisée. Le seul dispositif de protection est le pare-feu. Tous les serveurs et toutes les stations appartiennent au même réseau 172.20.100.0/23 (à noter que le /23 ne semble pas approprié car un /24 suffit à la lecture des ips utilisées ; un pirate opérant sur le réseau pourrait donc utiliser la plage restée vacante: 172.20.100.255-101.254) Aussi, la borne wifi offre un point d'entrée idéal sur le réseau pour un pirate. L'unicité du mot de passe et sa probable libre diffusion doit permettre de le trouver sans utiliser de technique de "hacking". Au pire, une attaque "brute de

Dans le cas [illegible] le WAF partir d[illegible]

Fin

force → permettra d'en venir à bout
Après intrusion, il sera difficile de trouver dans les logs des informations intéressantes car le mot de passe est identique pour tous.
Pour finir, l'accès à Internet par du NAT est très dangereux car il rend très difficile (voire impossible) la mise en place de filtrage vers des sites dangereux pour l'entreprise (phishing, hébergeur de virus, etc.)
Ensuite, un inventaire des systèmes et des applications est réalisé. Dans notre cas, il révèle de nombreuses failles de sécurité. Tout d'abord, on retrouve des OS dont le support est restreint voir interrompu:

- RedHat 4.5 (demande un contrat de maintenance particulier)
- Windows XP SP3 (non maintenu)
- Ubuntu 10.10 (non maintenu)

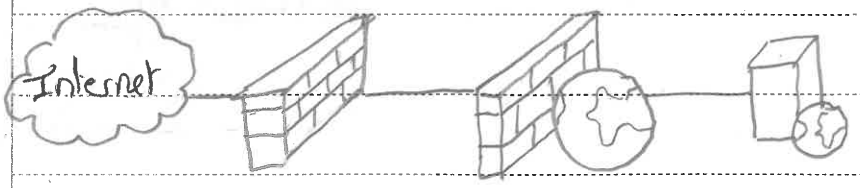
A noter que les autres OS ont déjà des versions plus récentes et qu'il faut donc déjà envisager leur mis à jour.
Ensuite, au niveau des applications, on remarque aussi des versions trop anciennes:

- Office 2010 (actuellement Office 365)
- LibreOffice 3.2 (actuellement LibreOffice 5.5)

2) Le Web Application Firewall est un pare-feu de niveau applicatif (niveau 7 du modèle OSI). Il permet donc de faire de l'inspection protocolaire sur les principaux protocoles du web : http(s), ftp(s), etc. Il se place généralement entre un pare-feu de niveau (3/4 voire IPS) et un serveur web. Grâce à des règles plus proches des applicatifs (Apache, mysql, Oracle, Postfix, ...), il est capable d'identifier des menaces évoluées comme l'injection SQL, le « script hacking » (failles AJAX), etc. Sa capacité à analyser les protocoles web a néanmoins des inconvénients. Malheureusement, ils sont difficiles à éviter car ils sont inhérents à son fonctionnement :

- Le WAF engendre de la latence. En effet, l'analyse des protocoles nécessitent de conséquentes ressources « processeur et mémoire ». Le temps de traitement pour valider toutes les règles ralentit le trafic. Le conseil est d'avoir un WAF très puissant en CPU et RAM.
- Le WAF doit déchiffrer le SSL. En effet, par définition, le SSL ne peut pas être analysé car il est chiffré. Cette opération a elle-même plusieurs inconvénients :
  - elle consomme des ressources machines
  - elle nécessite de placer les certificats serveurs sur le WAF
  - dans le cas d'une volonté de rechiffrement après le WAF, on a crée un « man-in-the-middle »

Dans le cas de l'architecture existante, il faut placer le WAF entre le pare-feu et les services accessibles à partir d'internet. Le schéma suivant montre son placement dans l'architecture :



Pare-feu WAF Serveur Web

3) La zone démilitarisée (DMZ) et le double bastion sont, pour ma part, des architectures plutôt complémentaires qu'opposables. Je m'explique :

- Le double bastion est la mise en place d'une double barrière de pare-feux. On utilise en général des équipements de marques différentes voire des technologie différentes (simple pare-feu, IDS, IPS, WAF, etc.)

- La DMZ est une zone de protection. Elle possède son propre adressage réseau et est obligatoirement protégée par un pare-feu. Seul les accès strictement nécessaires doivent être permis.

Les deux architectures ont un inconvénient commun : la latence. En effet, même minime, la latence générée par les pare-feux n'est pas nulle. Aussi, plus les équipements de sécurité font de l'inspection poussée, plus les débits sont allongés. L'autre inconvénient est le coût : il faut acheter un voire plusieurs pare-

ASSEMBLÉE NATIONALE

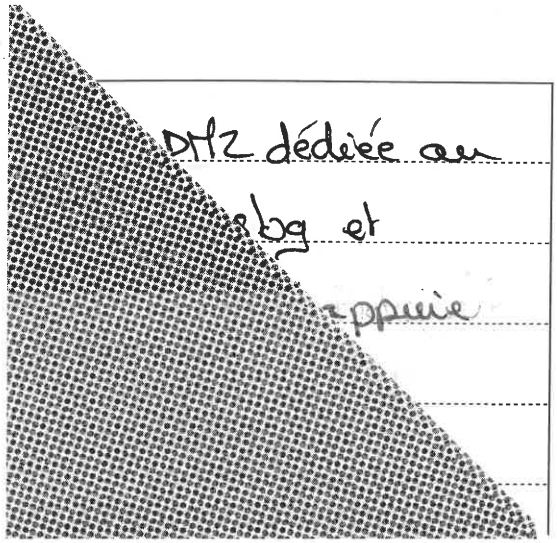
000212

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : PRODUCTION

Copie n° : 2 / 7



feux. Dans les deux cas, il faut aussi maîtriser les flux de l'entreprise :

- Pour le double bastions, les flux entreprise ↔ Internet
- Pour la DMZ, les flux. Internet ↔ DMZ
  . Internet ↔ Réseau d'entreprise
  . DMZ ↔ Réseau d'entreprise

Les avantages de ces deux architectures est d'accroître le niveau de sécurité :

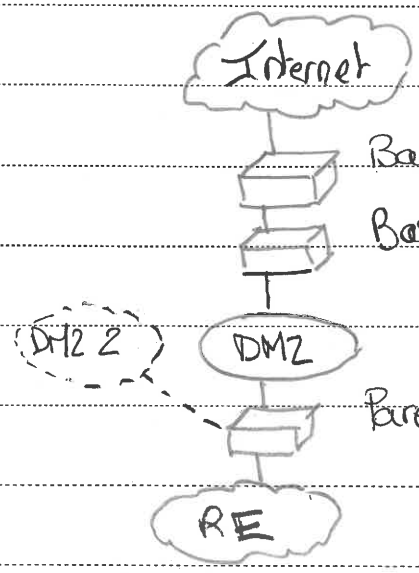
- Pour le double bastions, il protège des attaques ciblées sur un pare-feu (ou plutôt une technologie de pare-feu). Si le premier bastion tombe, le second doit résister.
- Pour la DMZ, la restriction fine des flux évite les attaques à la fois de l'intérieur et de l'extérieur en permettant que les accès strictement nécessaires (à noter que le double bastion est vulnérable aux attaques internes).

Donc, je vais proposer une architecture qui offre les avantages

000212

5) Un serveur
le port
com
d

des deux technologies :



DMZ : hébergement des serveurs
d'entrée et sortie internet
(web, relais de messagerie, etc.)

RE (Réseau d'entreprise) : stations de travail

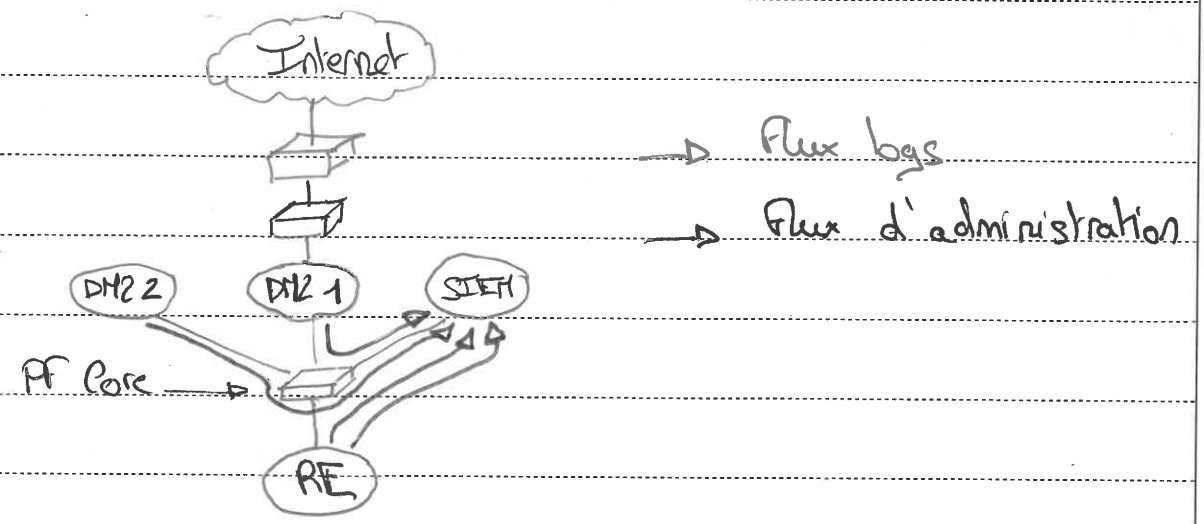
DMZ 2 (deuxième DMZ) : serveurs qui n'ont pas besoin d'accès
internet (AD, messagerie, etc.)

4) Le SIEM comme son nom l'indique est composée de deux composantes de base :

— Security Information : l'ensemble des "logs" pertinents du système d'information sont collectés sur des serveurs dédiés qui disposent d'une taille de stockage importante (servent connectés à un SAN)

— Event Management : Un moteur paramétrable en fonction des services et données de l'entreprise corrèle les "logs" pour fournir des informations et alertes de sécurité.

Dans notre cas, je propose de créer une DMZ dédiée au SIEM dans laquelle sera hébergée un cluster syslog et le cluster disposant du moteur de corrélation. Je m'appuie sur l'architecture proposée à la question 3. Cela donne



Donc dans mon architecture, les serveurs de la DMZ 1 et DMZ 2 envoient leurs logs via le pare-feu Core au SIEM. Les stations de travail equipées d'un eventuel agent SIEM comme NEXTHINK envoient leurs logs au SIEM. Seuls les administrateurs peuvent administrer les equipements du SIEM.

Sur un serveur Linux, il faut editer le fichier du syslog installé :

```
$ vim /etc/syslog-ng/syslog-ng.conf
$ :$        (→ aller à la fin du fichier)
$ *         <ip_du_serveur_siem> <port_du_serveur_siem>
```

5) Un serveur de messagerie est accessible en Telnet via le port d'écoute smtp (25). Je tape donc les commandes suivantes (de mémoire mais je vérifie sur Internet):

```
$ telnet 172.20.100.1 25
$ HELO
$ mailto john.doe@cna.fr
$ object (ou subject)
      mon message
$ bye
```

6) La commande nativement présente sur les systèmes d'exploitation libre (de type Linux) est iptables. Elle permet de paramétrer les fonctions firewall directement intégrées au noyau Linux.
Par exemple, je vais paramétrer le serveur de messagerie dont l'ip est 172.20.100.1.
Nous admettrons que les services présents sur le serveur écoutent sur les ports suivants:

- smtp ↔ 25
- pop ↔ 53
- ssh ↔ 22

Tout d'abord, paramettrons la police par défaut à DROP:

```
$ iptables -P -j DROP
```

Ensuite, paramettrons les règles par les ports

ASSEMBLÉE NATIONALE

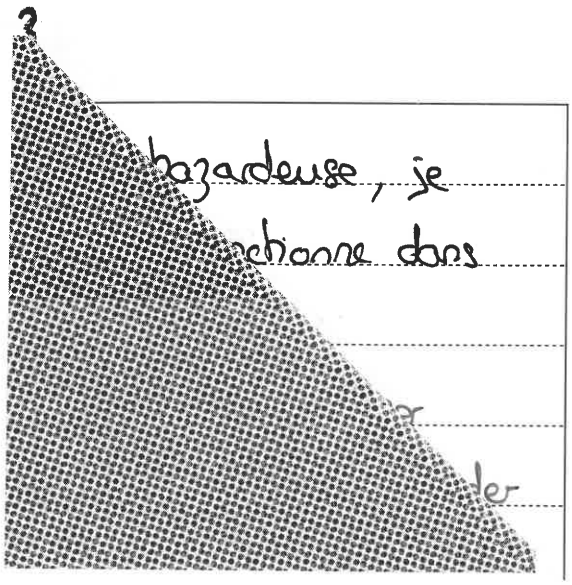
000212

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : PRODUCTION

Copie n° : 3 / 7




```
$ iptables -A PREROUTING -s 172.20.100.0/24 -d
    172.20.100.1 -dest-port 25 -j ACCEPT
$ iptables -A PREROUTING -s 172.20.100.0/24 -d
    172.20.100.1 -dest-port 53 -j ACCEPT
$ iptables -A PREROUTING -s 172.20.100.101 -d
    172.20.100.1 -dest-port 22 -j ACCEPT
```

N'étant pas certain des commandes, je détaille les commutateurs :

-A PREROUTING : operation realisée à l'arrivée du paquet

-s : ip source

-d : ip destination

-dest-port : port destination

-j ACCEPT : action réalisée (dans les 3 cas : ACCEPT)

Aussi, j'ai considéré que l'administrateur avait la station dont l'IP est 172.20.100.101

Volontairement (pour ne pas complexifier), j'ai permis l'accès aux services messagerie (SMTP et POP) aux stations et aux serveurs. Il faudrait les restreindre aux postes qui en ont besoin.

Dans ce cas, il f
Si une infra
votre envi
La co
est
p

Le schéma des accès :

ACCEPT:

172.20.100.0/24 → 25, 53

172.20.100.101 → 22

défaut : BLOCK

7) Le principal conseil à lui donner est de fournir une infrastructure virtualisée qui sera transparente pour l'utilisateur. Je m'explique : L'utilisateur doit conserver le niveau de service d'avant la virtualisation. Donc, le premier élément à étudier est le besoin en performance des futures "Virtual Machines". Pour cela, il doit mettre en place des sondes sur les serveurs existants et ensuite analyser les ressources nécessaires par VM. Une fois l'étape de « sizing » effectuée, il faut choisir le système de virtualisation et acheter les hyperviseurs pour supporter l'infrastructure. Pour la technologie de virtualisation, il faudra étudier le ratio coût/administration (l'opensource est possible avec des équipes formées ; les systèmes propriétaires sont plus faciles à gérer mais aussi plus coûteux). Quand les choix sont faits et les serveurs achetés, il faut étudier la migration des serveurs. Il existe alors deux principales solutions :

- réinstallation des serveurs sous forme de VMs
- conversion de physique à virtuel des serveurs

Même si la deuxième solution apparaît encore hazardeuse, je peux garantir de ma propre expérience qu'elle fonctionne dans la quasi-totalité des cas.
Il va devoir aussi intégrer un autre paramètre : virtualiser les serveurs d'un SI implique nécessairement d'appréhender la virtualisation des réseaux. C'est peut-être le plus difficile donc il ne faut pas le négliger. Une formation sera évidemment nécessaire pour les administrateurs mais elle devra être plus poussée pour l'architecte.
Il faut aussi être conscient d'un inconvénient lié aux environements virtualisés : un hyperviseur qui tombe, c'est possiblement une dixaine de VMs arrêtées. Dans le cas de la virtualisation, il est plus que jamais impératif de redonder les VMs et il faut nécessairement au moins deux hyperviseurs.
Dernier conseil, dans le cas d'un incident, rester calme et faire des schémas. La virtualisation ajoute une couche de complexité au SI. Il faut être méthodique pour la résolution des incidents.

8) Dans le cas d'un environement Active Directory, on peut aisément envisager créer un domaine de test au sein de la même forêt que la production c'est tout à fait possible mais les administrateurs de l'AD peuvent refuser.

Dans ce cas, il faut créer un environnement isolé et dédié.
Si une infrastructure virtualisée existe, elle pourra hébergée votre environnement de test.
La commande utilisée pour creer un nouveau domaine est DCPROMO mais depuis les environnements 2012 tout peut être effectué à l'aide de l'outil de management du serveur.
Ainsi, pour ma part, j'utilise l'outil graphique qui permet les configurations suivantes :

- gestion des rôles
- configuration du DNS / DHCP (dynamique DNS)
- activation des fonctionnalités (impression, fichier, IIS, ...)

Le resultat du passage d'un serveur à contrôleur de domaine est par défaut :

- authentification obligatoire avec des comptes du domaine
- serveur DNS (porteur des enregistrements de l'infrastructe)
- racine du système de fichiers distribué (DFRS)
- porteur des polices de securité (GPO)
- serveur kerberos
- annuaire ldap

9) L'analyse de risque a pour but d'evaluer la faisabilité d'un projet au sein d'un SI. Elle permet d'identifier à partir d'une liste de critères prédéfinis si l'environnement est apte

ASSEMBLÉE NATIONALE

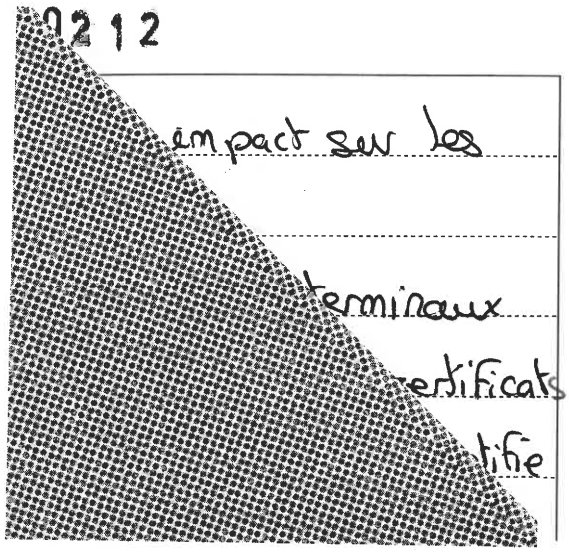
000212

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : PRODUCTION

Copie n° : 4 / 7



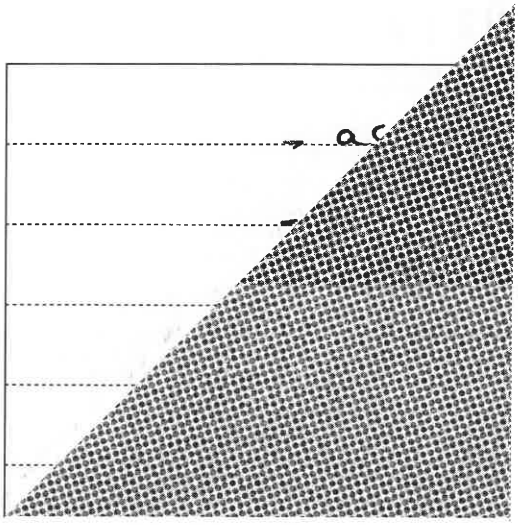
à accueillir la nouvelle architecture. Elle peut mener à la non realisation du projet mais peut aussi fixer une liste de travaux à réaliser pour adapter le SI. Elle est par conséquent ré-évaluable. Il faut etudier les aspects réseaux, systèmes et de sécurité. Un recencement de l'existant est nécessaire pour ensuite produire le rapport d'analyse de risques. Les mécanismes organisationnels sont aussi pris en compte.

1a) Création d'un compte utilisateur :

Le SI ne disposant pas dans l'immédiat d'un outil informatisé de création d'un nouvel utilisateur, le processus est pseudo automatisé :

- envoie par les RH de l'identité du nouvel arrivant ainsi que son poste dans la société aux services suivants :
  - AD
  - Messagerie
  - Gestionnaire d'applications

000212



- Création du compte AD par le service AD et affectation des groupes
- Création de la boîte aux lettres par l'équipe messagerie
- Création des autorisations d'accès aux applications par les gestionnaires d'applications
- configuration de la station de travail par un informaticien de proximité
- transmission d'une fiche explicative au nouvel arrivant

Mise à jour des ordinateurs du parc bureautique :

- l'ordinateur est installé avec une clé publique du serveur de collecte
- chaque nuit, à 0100, le serveur de collecte scanne le réseau à la découverte de nouveau ordinateur
- si nouvel ordinateur, il l'insère dans la base de collecte
- le scan matériel et logiciel de l'ordinateur est effectué
- le fichier de collecte est traduit en base de données
- les informations sont disponibles dans l'interface graphique

11) Pour sécuriser le WIFI tout en minimisant l'impact sur les utilisateurs, je préconise l'architecture suivante :

- Un SSID (et un vlan dédié) aux ordinateurs et terminaux de l'entreprise qui s'appuie sur l'utilisation de certificats (ou jetons cryptographiques). Le poste ou le terminal s'identifie ainsi automatiquement de manière sécurisé. La navigation peut être tracée grâce au certificat. Un dispositif de certificats autosignés peut être utilisé (pour éviter les contraintes des PKIs)
- Un SSID (et un vlan dédié) pour les terminaux des visiteurs. Dans ce cas un portail d'enregistrement est nécessaire et l'utilisateur doit saisir une adresse de courriel valide. Il peut uniquement accéder à Internet et aux ressources choisies par l'entreprise. Sa navigation est tracée.

12) La sécurisation des switchs peut être réalisée ainsi :

- niveau 2 :
  - accès d'administration en SSH avec une clé dsa/rsa
  - Filtrage par MAC
  - Shutdown des ports inutilisés
  - un port ne possède que les VLANS nécessaires

  ex port 1/0/1 - port access VLAN 90 - mac-authorized xx:xx:xx:xx:xx:xx
- niveau 3 :

- accès d'administration en SSH avec une clé dsa/rsa
- ACL en définissant les réseaux sur un port (anti spoofing)
- shutdown des ports non utilisés

ex port 1/0/1 - network-authorized 172.20.100.0/24

Pour ma part, une bonne solution est de remplacer les routeurs (ou switch niveau 3) par des pare-feux.

13) La collecte sera réalisée à l'aide d'un script bash (cela à l'avantage de pouvoir être appliqué à Windows avec Cygwin) et de connexions SSH (utilisation de clés pour la collecte).

- ssh user_collecte@ip_ordinateur "sh collecte.sh >> /ipordinateur.txt"
- collecte.sh :
  - w # utilisateurs connectés
  - ps -ef # processus exécutés sur la machine
  - last | head -n 200 # 200 dernières connexions
  - netstat -n | grep -i udp | grep -i active # UDP actifs
  - netstat -n | grep -i tcp | grep -i listen # TCP écoute
  - netstat -n | grep -i tcp | grep -i active # TCP actifs
  - df -h # liste et taille des partitions

ASSEMBLÉE NATIONALE

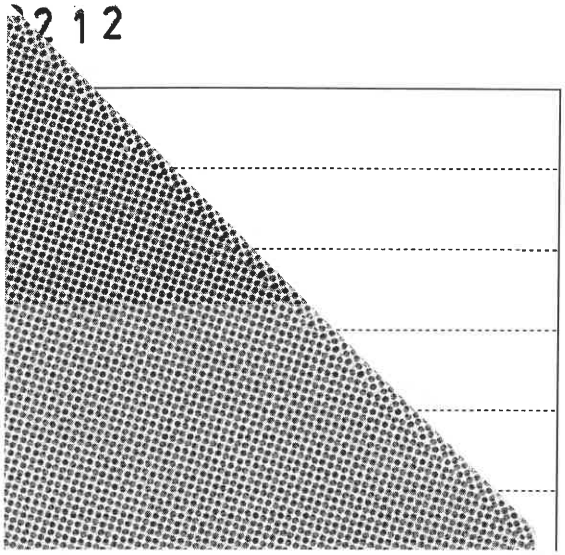
000212

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : PRODUCTION

Copie n° : 5 / 7



- scp user_collecte@ip_ordinateur:/ipordinateur.txt /srv/ipordinateur/ipordinateur.txt
- scp -r user_collecte@ip_ordinateur:/var/log/* /srv/ipordinateur/log/

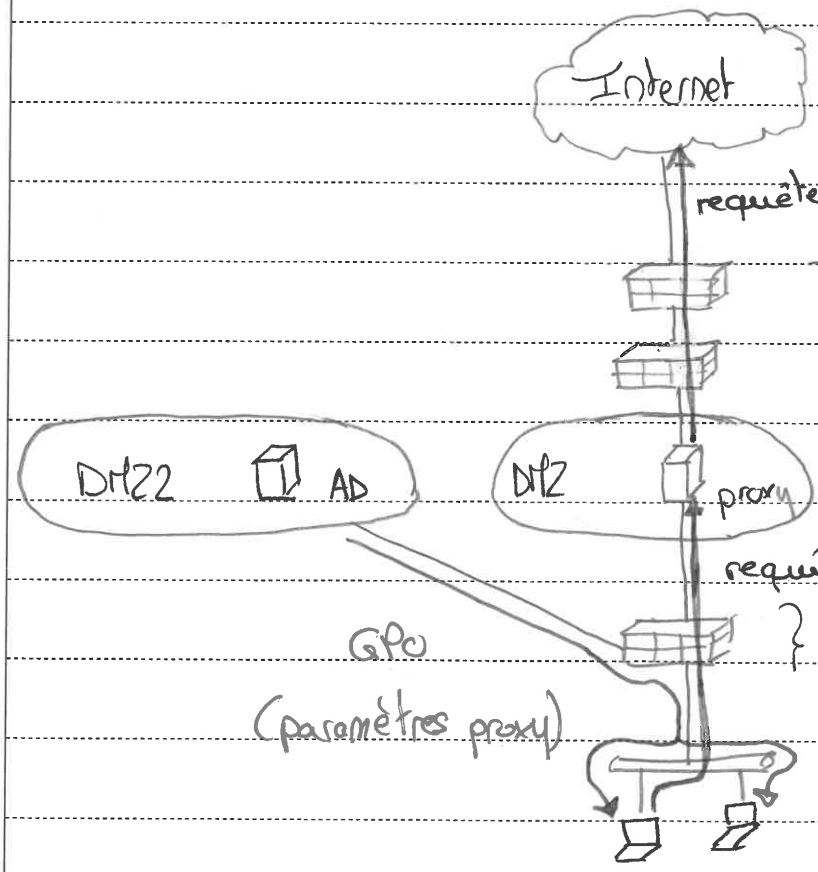
→ récuperation des logs sur le serveur de collecte

14) Dans le contexte actuel de piratage à l'aide des techniques de phishing, il est nécessaire de filtrer l'accès à Internet. La solution par NAT n'est nativement pas prévue pour gérer des listes d'exclusions dynamiques. Elles sont pourtant nécessaires pour éviter l'accès à des sites dangereux d'un utilisateur. La liste de ces sites évoluant sans cesse, il faut un dispositif qui se mettent à jour automatiquement. Cette fonctionnalité est assurer par les serveurs proxy. Ils permettent en fonction de la stratégie de l'entreprise de restreindre l'accès à des catégories de sites (jeux, pornographie, crime, etc.). Par soucis de sécurité forte, on peut même refuser l'accès aux sites qui

ne seraient pas catégoriser

Je propose donc une architecture à base de proxy et de déploiement des paramètres proxy par GPO.

Schéma de l'architecture



ASSEMBLÉE NATIONALE

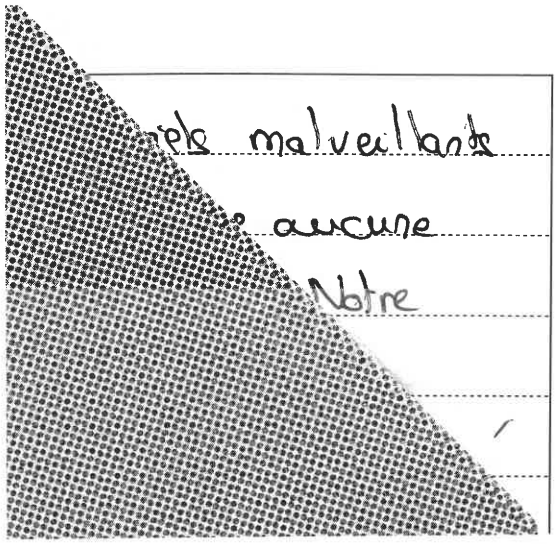
000212

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : PRODUCTION

Copie n° : 6 / 7



2 eme PARTIE

le 30/05/2017

à PARIS

Objet Etat des lieux de l'infrastructure et propositions

Références Annexe 1 et 2 (documents fournis)
Annexe 3 (à la fin)

Monsieur le Directeur,

Dans le cadre du renouvelement du marché passé avec l'administration et suite au récent piratage, vous m'avez missionné pour effectuer un état des lieux de notre système d'information et pour ensuite vous proposer des évolutions.

000212

Nous risquons p
OS et appli
Nul
es

Mon analyse a permis de montrer que notre SI est pour de nombreuses raisons autant systèmes que réseaux et applicatives vulnérable aux attaques malveillantes. Je vais vous les détailler en deux grandes catégories : les faiblesses de notre infrastructure réseau et les vulnérabilités systèmes. Ensuite, je vous présenterai mes propositions d'évolution.

Tout d'abord, même si notre réseau est fonctionnel, il n'est pas securisé. Il est vulnérable de l'intérieur et de l'extérieur.

Au sein de notre infrastructure, toutes les machines sont visibles et peuvent directement communiquer entre elles. De n'importe quelle station, un piratage est possible. Même si les serveurs sont protégés par des mots de passe, il est possible de lancer des attaques pour les surcharger. Ce problème est aggravé par l'existence d'un accès wifi qui arrive directement au sein de notre SI. Une démonstration de hacking de wifi vous montrerait comment il est facile de passer la securité des réseaux sans fils.

Ensuite, notre accès internet est un vrai problème. Mon analyse a montré qu'il est en partie responsable du dernier piratage

Les techniques de piratage utilisant des courriels malveillants ne cessent de croître. Notre système actuel n'offre aucune protection. Un simple exemple permet de comprendre. Notre service financier reçoit un courriel d'un de nos fournisseurs qui lui envoie une facture. Il l'ouvre. Il n'ont pas vu qu'à une lettre près, le nom est différent. Mais, trop tard, leur poste est infecté et un pirate est déjà en train de nous hacker.

Ensuite, une grande partie de nos systèmes d'exploitation et services applicatifs sont vulnérables à des failles à cause de l'absence de politique de mise à jour.

Premièrement, une partie de nos systèmes ne sont plus supportés par leur concepteur. Cela implique qu'ils ne sont pas mis à jour et qu'ils sont donc vulnérables à une partie des failles découvertes depuis la fin de leur support. C'est le cas des postes Windows XP. Fait aggravant, il s'agit des postes de gestion de la pare qui peuvent demain être victime d'une attaque. Imaginez les conséquences internes.

Deuxièmement, une autre partie de notre parc fonctionne sur des systèmes d'exploitation en fin de vie. Leur remplacement n'a pas débuté alors que le constructeur préconise leur mise à jour.

Nous risquons par conséquent d'amplifier le problème des OS et applicatifs non supportés.

Nul ne peut contester le fait que notre système d'information est actuellement très vulnérable à la vue des arguments exposés. Néanmoins, il est possible d'y remedier en réorganisant notre infrastructure réseau et en créant une politique de mise à jour.

Tout d'abord, je propose de réorganiser notre réseau en le segmentant et en mettant en place un service "proxy".

Premièrement, je propose d'opérer une segmentation entre le wifi visiteurs et le notre. Les deux reseaux doivent être étanches et ne laisser traverser que les services voulus. La mise en place de plusieurs pare-feux ainsi que de plusieurs zones est aussi nécessaire au sein de notre propre réseau d'entreprise. Ainsi, je propose que soit créé deux zones protégées : une pour les serveurs ayant accès ou étant accessibles d'Internet comme le serveur web, une seconde pour les serveurs d'infrastructure comme le serveur AD. (voir annexe 3 à la fin)

Deuxièmement, je suggère la mise en place d'un serveur proxy qui permettra de filtrer les accès à Internet

ASSEMBLÉE NATIONALE

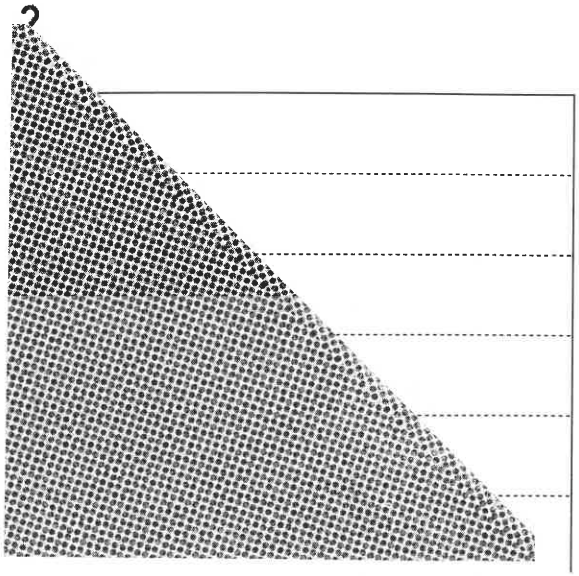
000212

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : PRODUCTION

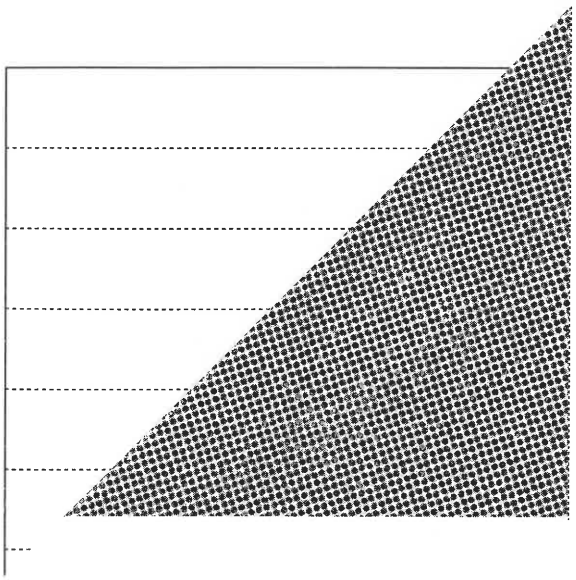
Copie n° : 7 / 7



Ainsi, il sera possible d'éviter l'accès aux sites dangereux et permettre l'accès qu'aux sites légitimes. A la vue de notre récent piratage, je préconise aussi le blocage des sites non catégorisés.

Ensuite, l'obsolescence de nos systèmes d'exploitation et applications est cette un moyen de piratage à partir du web mais également à partir d'une simple clé usb infectée.

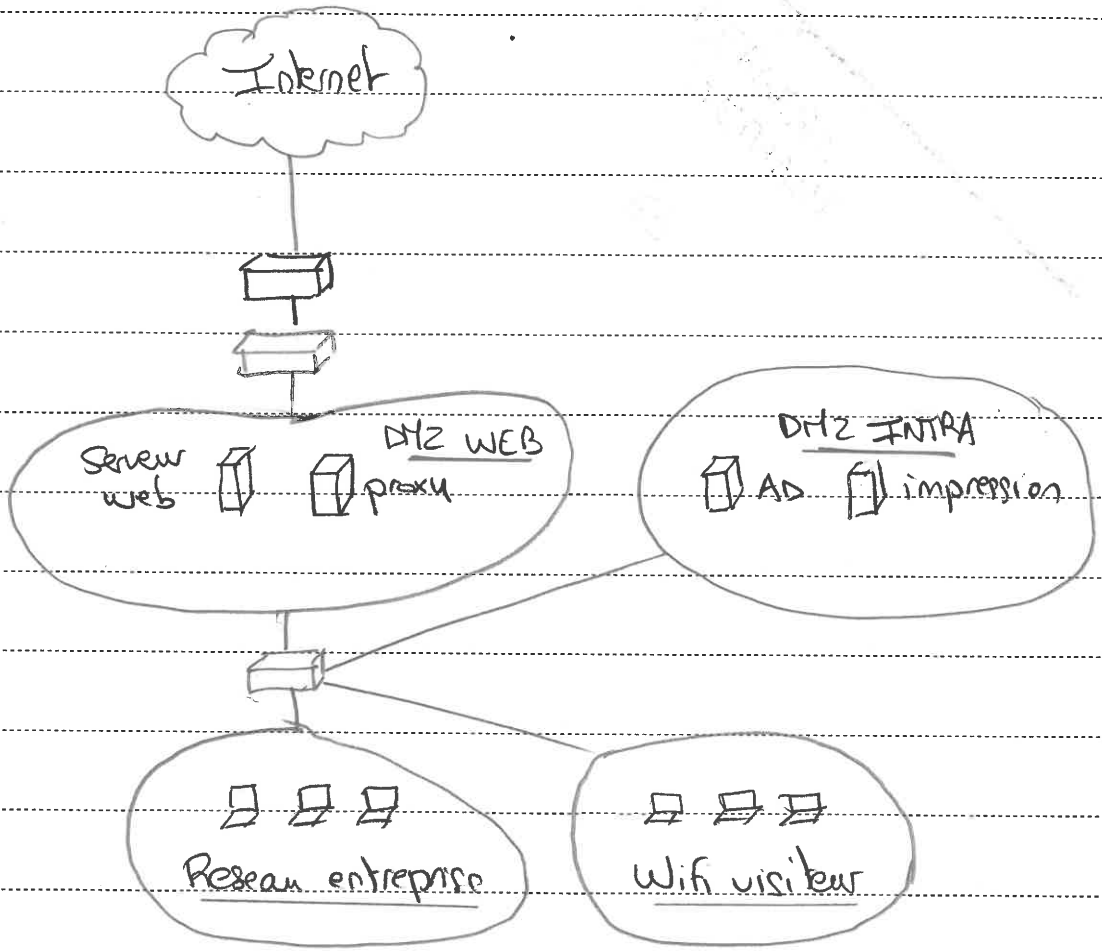
Je propose donc la mise en place d'une politique de mise à jour des systèmes. En amont d'une obsolescence, les nouvelles versions doivent être testées et validées. Avant la fin du support, le déploiement doit être effectué. Si une application n'est pas compatible avec le nouveau système, son remplacement doit être étudié. Si cela n'est pas possible, il faut s'orienter vers des logiciels de virtualisations applicatives.



Je suggère qu'en accompagnement de la politique de mise à jour soit mis en place un logiciel d'inventaire qui permettra de suivre les versions des OS et applications du parc informatique.

Pour conclure, notre système d'information est effectivement très vulnérable mais en réalisant mes préconisations nous parviendront à un environnement suffisamment sécurisé pour faire face aux attaques informatiques actuelles. Nous serons ainsi mieux préparé pour gagner le marché de renouvellement.

Annexe 3


Internet
DMZ WEB
Serveur web
proxy
DMZ INTRA
AD
impression
Réseau entreprise
Wifi visiteur

400005

ASSEMBLÉE NATIONALE

NOTE : 16,5 /20

Concours : INFORMATICIEN

Épreuve : TECHNIQUE

Copie n° : 1 / 3

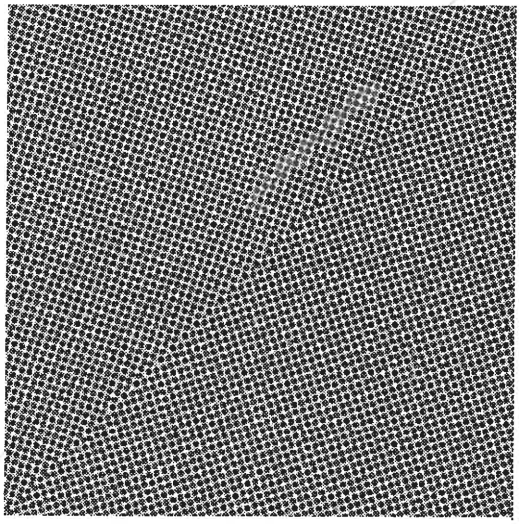
1. DNS Poisoning

Le DNS Poisoning est une attaque qui consiste à envoyer à un serveur DNS des réponses erronées. Il fournet alors aux clients des enregistrements faux qui peuvent les conduire sur des sites malveillants. Une des techniques de base est de surcharger un service DNS (Denis de service) et ensuite d'envoyer les réponses à sa place.

Pour identifier les enregistrements inexactes, le plus simple est de demander aux serveurs DNS d'écrire leur cache dans un fichier. La commande "rndc dumpdb" permet ainsi d'écrire le cache dans un fichier généralement placé sous /var/lib/named/data. Par script, il est alors possible de vérifier les enregistrements. La commande "dig" peut alors être utilisée pour effectuer la vérification :

dig @8.8.8.8 $nom_de_l_enregistrement.

En parallèle, il faut vider le cache des serveurs WEB et applicatif quand il existe. Sur un serveur Windows, il faut faire un "ipconfig /flushdns". Sur un Linux,



le redémarrage du service resolvconf doit suffire. L'impact sur le système d'information peut être très grave ... Imaginons que l'enregistrement correspondant à un relais smtp soit modifié, vous allez diriger une partie des messages vers un relais d'un pirate qui pourra lire des messages importants de l'entreprise.

2 Rebasculement réseau

Deux causes principales peuvent être à l'origine d'un trafic ARP important et croissant :

- dysfonctionnement du réseau comme une boucle dans un réseau sans Spanning-tree
- attaque ARP (ARP spoofing et poisoning)

Dans les deux cas, il faut identifier le segment du réseau qui est impacté. C'est là où se situe fort probablement l'attaquant ou l'équipement à l'origine de la boucle. Pour remédier à la diffusion des requêtes, le plus simple est d'isoler le tronçon d'où part les requêtes. Pour cela, nous nous servons des outils de supervision et

observons les trafics anormaux sur les ports des commutateurs et des routeurs. Pour isoler, il faut à partir du réseau d'administration, effectuer un « shutdown » du port d'un équipement en cause. Si on observe une diminution du trafic ARP sur le reste du réseau, c'est que l'origine a été circonscrit. En agissant alors pas à pas, on identifie ainsi, l'équipement ou le poste responsable.
Pour y remédier à long terme, il est possible de mettre en place : - le spanning tree pour éviter les boucles
- des dispositifs de sécurité sur les ports des commutateurs comme des ACL ou de l'affectation MAC

3. Logiciel malveillant distribué par messagerie

Comme il s'agit d'un logiciel malveillant qui pointe vers un site web, une bonne méthode est de recenser les postes qui ont été interrogés le site web malveillant. Une requête sur les serveurs proxy de l'entreprise donne ainsi une liste assez précise des postes touchés. Aussi, comme le logiciel a réussi à passer les dispositifs de sécurité de la messagerie, on peut facilement imaginer qu'il ne sera pas détecté par les antivirus des postes. On effectue néanmoins un contrôle au cas où l'antivirus local aurait identifier une attaque.

Dans tous les cas, si le fichier portant le virus n'est pas polymorphe, on le place dans les fichier à identifier et à mettre en quarantaine par l'antivirus des stations. Très vite, on obtient une liste des détections par l'antivirus.
On a donc deux listes finales :

- les stations qui ont requêtées vers le site malveillant (données en provenance des proxy)
- les stations que l'antivirus a détecté (après renseignement du fichier dans sa base antivirale)

Une fois les postes identifiés, ils sont éteints et un personnel informatique les redémarre déconnectés du réseau pour tenter une désinfection.
Outre cette mesure, il faut également interdire l'accès au site malveillant dans les serveurs proxy.
Pour éviter ce genre d'attaque, un outil de "sandboxing" peut être acheté.

4 A Lenteurs sur une nouvelle application identifiées par les utilisateurs

L'application est conçue sur le schéma n-tiers (dans notre cas 3 tiers : client ↔ serveur web ↔ SGBD). On peut donc déjà noter les causes inhérentes à ce type d'architecture :

ASSEMBLÉE NATIONALE

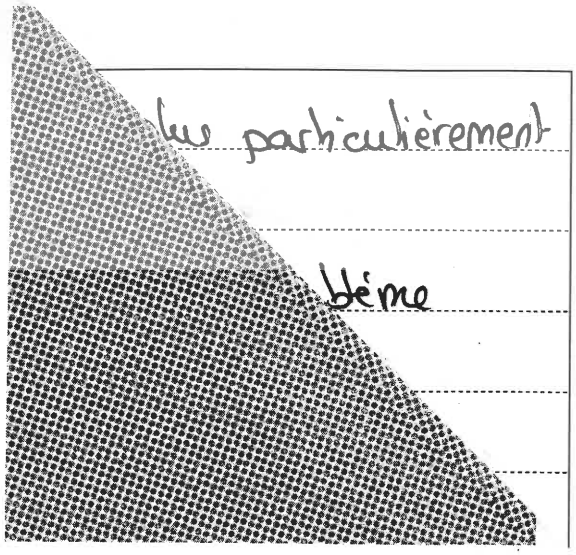
400005

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : TECHNIQUE

Copie n° : 2 / 3



- ressources matérielles des serveurs (voire client)
- dysfonctionnements "réseau" (segment client↔Web ou Web↔SGBD)
- applications non optimisées (trop de requêtes SGBD)
  mal codées (ressources non existantes)

Pour identifier les problématiques de ressources matérielles, la commande "top" est la plus appropriée. Elle permet de voir le taux d'utilisation CPU et de la RAM. Elle montre également les processus les plus gourmands. Pour la station (si windows), on peut utiliser le moniteur de performances.

Pour détecter les dysfonctionnements "réseau", il faut tout d'abord regarder l'état des interfaces des différents équipements. Pour Linux, plusieurs commandes peuvent nous aider : ip address show, ip link show, ethtool et mii-tool. Deux éléments sont à observer, la vitesse de l'interface et les erreurs de transmission. Pour windows, il faut aller dans les propriétés de la carte réseau.

Finalement, il faut rechercher les causes liées à l'application.

Les utilisateurs a
perdent egale

5.B
Le

Elle représente 80 % des dysfonctionnement des systèmes d'information. Un nombre de requêtes trop élevées vers le SGBD est souvent la première cause. Les outils tcpdump (capture de paquets) et wireshark (lecture de fichiers dump) permettent ainsi de démontrer le problème.
Enfin, les fichiers de log doivent être observés pour rechercher les difficultés d'accès aux ressources, les "timeouts", les erreurs de codage, ...

4.B Erreur 404

Ce code signifie que la page demandée est introuvable.
Dans les faits, cela ne veut pas dire qu'elle n'existe pas. Il peut y avoir un problème de droit qui empêche le serveur de lire la page.
Donc pour déterminer la source de l'erreur, il faut réaliser deux opérations :

- rechercher le chemin réel de la ressource et vérifier son existance
- vérifier si le serveur WEB a les autorisations nécessaires pour renvoyer la page

Tout d'abord, pour déterminer le chemin réel, il faut lire les

fichiers de configuration du serveur WEB et plus particulièrement les alias et virtuelhost.
Si la ressource est absente, il faut retourner le problème au développeur
Si la ressource est présente mais que le serveur WEB ne peut retourner la page, il faut vérifier les autorisations des dossiers et fichiers. Il est possible d'utiliser la commande << su >> pour se substituer au serveur WEB.

5.A Borne WIFI installée sans autorisation

Mise à part les problématiques d'affectation des canaux WIFI liées au voisinage de plusieurs bornes, le vrai problème est l'activation du DHCP sur l'interface physique. Le service DHCP est d'une conception très simple. Il doit être unique sur un segment du réseau. Dès qu'un DHCP reçoit une requête, il répond au client en lui fournissant une IP. Dans notre cas, si la borne répond en premier, elle fournira une IP de sa plage affectable au client. Si la borne est bien configurée, elle peut effectuer un routage vers les autres ressources. Il peut être, dans ce cas, difficile d'identifier sa présence. Les utilisateurs se plaindront alors de lenteurs et de problèmes d'accès aux ressources fournies au travers du réseau. En cas de mauvaise configuration de la borne, l'accès aux ressources peut être totalement impossible.

des utilisateurs qui doivent avoir une IP statique perdant également l'accès à leurs ressources spécifiques.

5.B Identification de la borne

Les perturbations peuvent être difficile à identifier. Il faut que le personnel informatique vérifie l'adressage de la station cliente. Si l'IP n'appartient pas au "range" de l'entreprise, il y a probablement un deuxième serveur DHCP sur le réseau.

Grâce à un "nmap" ou équivalent sur le poste, on identifie les equipements connectés. La passerelle réseau est certainement la borne. On peut ensuite pour l'identifier, utiliser la commande arping et récupérer son adresse MAC. On retrouvera ainsi le constructeur de la carte réseau et peut être la marque de la borne. Un nmap plus poussé sur la borne peut nous renseigner sur les services présents.

Le plus simple reste d'utiliser un navigateur et de saisir : http://ipdelaborne

ou " /admin

Fort probablement, on trouvera l'interface de la borne (sa marque et sa version)

400005

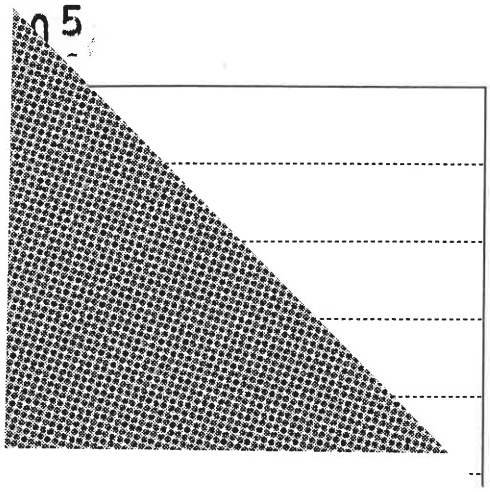
ASSEMBLÉE NATIONALE

NOTE : ..... /20

Concours : INFORMATICIEN

Épreuve : TECHNIQUE

Copie n° : 3 / 3



6. Problème nfs

L'erreur NFS est classique dans notre cas:
le serveur NFS ne donne pas les autorisations au client car le client n'est pas présenté en user-1 ou user-2. Il n'est ni présent dans son fichier "hosts" ni présent dans le DNS

Il faudrait rajouter sur le serveur
10.3.3.x user-1
ou
user-2

ou il faudrait entrer les informations dans le DNS