MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

ANNALES DU CONCOURS

Accès au corps des attachés de la DGSE

Épreuve d'admissibilité :
spécialité sciences et technologie - informatique

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Session 2021

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

3ème épreuve d'admissibilité

Spécialité : sciences et technologie - informatique

Épreuve consistant à répondre à une série de questions portant sur la spécialité « Sciences et technologie - Informatique ».
Il est demandé au candidat de démontrer les étapes de son raisonnement en exploitant les documents du dossier comprenant dix pages maximum et en faisant appel à ses connaissances personnelles.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Durée : 4 heures - coefficient 8

CONCOURS EXTERNE
POUR L'ACCÈS AU CORPS DES ATTACHÉS

SESSION 2021

<u>Epreuve d'admissibilité</u> :

Spécialité : Sciences et technologie - Informatique

Épreuve consistant à répondre à une série de questions portant sur la spécialité **« Sciences et technologie – Informatique ».** Il est demandé au candidat de démontrer les étapes de son raisonnement en exploitant les documents du dossier comprenant dix pages maximum et en faisant appel à ses connaissances personnelles.

Durée : 4 heures ; coefficient 8

Red Team & Blue Team

0. Ce sujet a pour objectif de tester un éventail large des connaissances en informatique du candidat.
1. L'orientation Cyber/SSI du sujet est assumée, mais ne constitue pas un prérequis .
2. En ce sens, les thématiques abordées sont vastes et relèvent des connaissances acquises lors de l'exploitation d'un système d'informations (SI).
3. Peu de questions « dites à tiroir » sont présentes afin de permettre au candidat de rebondir si nécessaire .
4. Le candidat est invité à traiter dans l'ordre qu'il souhaite les deux parties du sujet, qui sont totalement indépendantes.
5. Toute réponse sera argumentée et justifiée .

---

6. Les équipes rouges ont été développées pour mimer les techniques des attaquants et exploiter les failles d'un SI.
7. Les équipes bleues ont été créées pour concevoir des mesures de défense contre de telles activités.

Blue Team (35 points)

Cette partie aura pour objectif de concevoir et maintenir une infrastructure de production sécurisée

Contexte : Vous faites partie de l'équipe de sécurité de l'entreprise *Eaupuredotcom*.

Eléments en votre possession :

- Eléments administratifs :
  - La société *Eaupuredotcom* travaille dans le domaine du contrôle de la qualité des réseaux d'eau potable. En tant que sous-traitant des grands groupes de distribution d'eau du robinet, elle a pour mission de vérifier en temps réel la potabilité de l'eau et d'agir via l'injection de divers produits dans les réseaux d'eau afin de maintenir cette potabilité. Elle travaille à son tour avec des sous-traitants.
- Eléments techniques
  - Internet
    - URL du site web : *https://eaupure.com*
    - Pare-feu commercial Netask
    - Portail web IIS
    - SGBD MS-SQL
    - Les données statiques sont stockées sur un CDN.
  - Périmètre réglementaire :
    - *Eaupuredotcom* est un OIV.
  - Intranet
    - Une forêt Active Directory (AD) qui porte la base de comptes, d'objets et assure les fonctions d'authentification, d'autorisations.
    - Un SAN constructeur porte l'ensemble des données utilisateurs.
  - Postes clients

- Globalement : Les services disposent de postes Windows 10 intégrés au domaine.
- Exceptions :
    - Le service reprographie dispose de postes Windows 7, dernière version compatible avec le progiciel métier.
    - Le service développement dispose de postes Linux.
    - L'équipe de sécurité dispose de postes Windows et linux.

1. Sécurité organisationnelle (5,5 points)

1. Eléments non-informatiques (2,5 points)
    a. Que signifie être un *OIV* ?
    b. Quelles en sont les implications pour l'entreprise ?
    c. Indiquez le nom de l'organisme de contrôle.
2. Eléments informatiques (3 points)
    a. Quels sont les risques techniques induits par le recours à une prestation de service (Trois lignes max.) ?
    b. Citez deux contre-mesures que vous seriez susceptible d'appliquer afin de réduire ces risques ?

2. Sécurité Internet (12 points)

a. Cryptographie (8,5 points)
    i. Site internet
        1. Que signifie le s de https ?
        2. Pouvez-vous détailler le protocole utilisé ? (Cinq lignes max.)
        3. Quelle est la dernière version de ce protocole ? Qu'apporte-elle par rapport aux version précédentes ?
        4. Citez au moins deux failles de ce protocole.
    ii. Quel est le référentiel français fixant les règles de sécurité de l'information pour les échanges entre les usagers et l'administration ?
    iii. Le serveur web utilise un certificat.
        1. Citez trois attributs de ce certificat et leur usage.
        2. Qu'est-ce qu'une chaine de certification ?
        3. Citez deux types d'alertes de sécurité qu'un navigateur peut rencontrer.
        4. Schématisez l'échange qui s'établit entre le client et le serveur lors de la connexion au site web (https) en spécifiant les différents mécanismes cryptographiques et les phases en clair.

b. Développement (3,5 points)

Le site web dispose d'un mécanisme d'authentification pour offrir un espace personnel aux utilisateurs.

i. Qu'est-ce qu'une injection SQL ?
Rédigez en une ligne une requête générant une telle injection.

Une partie du code utilisé pour l'authentification est :

```
1   #include <stdio.h>
2   #include<string.h>
3
4   void  auth(char *str)
5           {
6           char buf[32] ;
7           strcpy(buf,str) ;
8           }
9
10  int main(int argc, char *argv[])
11          {
12          if (argc > 1)
13                  {
14                  auth(argv[1]) ;
15                  }
16          return 0 ;
17          }
```

ii. Comment se nomme ce type de vulnérabilité ?
iii. Quelle sera le message d'erreur lorsque la vulnérabilité sera été exploitée.
iv. Indiquez, dans le code précédent comment corriger cette vulnérabilité en réécrivant la ou les seules lignes nécessaires.

3. Sécurité Intranet (12,5 points)

a. Active Directory (AD) (1,5 points)
   i. Qu'est-ce que le niveau fonctionnel d'un AD ?
      1. Donnez un exemple (Deux lignes max.) illustrant l'intérêt de l'augmenter.
   ii. Qu'est-elle l'utilité d'une extension de schéma AD ?

b. Réseau (3 points)
   i. Identifiez trois mesures de protection à appliquer au niveau des réseaux de desserte et indiquez pour chacune la menace contre laquelle elle permet de se prémunir. (Trois lignes maximum pour chaque réponse)

c. Postes clients (6,5 points)
   i. Clients Windows
      1. En orientant votre exposé sur les seules fonctions de sécurité et d'architecture, expliquez (dix lignes max) les évolutions réalisées sur Windows 10.
   ii. Clients Linux
      1. Proposez six mesures à mettre en œuvre sur les postes Linux de l'équipe d'administration afin d'améliorer le niveau global de sécurité du SI.
         - Pour chacune d'entre elles, indiquez dans un tableau en les classant les par ordre de priorité d'application selon le gain en sécurité (*MIRE* : Minimal / Intermédiaire/Renforcé/Elevé) si vous deviez en préconiser l'application. Indiquez les éventuelles difficultés de mise en œuvre sur une échelle de --- à +++.

d. Protocoles d'authentification (1,5 points)
   Ce protocole doit fournir un mécanisme de SSO.
   i. Quel protocole d'authentification serait le plus adapté dans cette infrastructure ?

ii. Réalisez un schéma synthétique de l'échange protocolaire réalisé lors l'authentification d'un client quelconque auprès d'un service tiers, type site web de l'entreprise.

4. Infrastructure (5 points)

a. Cas concret en DSI (5 points)

Proposez en vingt lignes maximum (ou quinze lignes et un schéma) une solution de votre choix (libre ou industrielle) en prenant en compte les impacts financiers, d'extensibilité, techniques, RH et enfin la conduite du changement, sur l'une ou l'autre des deux thématiques suivantes :

- Stockage
- Virtualisation

Red Team (25 points)

Cette partie aura pour objectif de concevoir et réaliser une intrusion sur un système.

Vous êtes contacté par une société pour réaliser l'audit boite noire de son système informatique.

Eléments en votre possession :

- Eléments administratifs :
  - Société : *Target.Inc*
  - Point de contact : M. Guillaume Portails, PDG de *Target.Inc*, le client
  - Activité de *TargetInc* : Prestataire de service informatique pour des grands groupes industriels.
- Eléments techniques
  - Numéro d'AS : 1982
  - URL du site web *https://www.targetinc.com*

1. Préalable (5 points)

1. Eléments non-informatiques (4 points)
   a. Identifiez et détaillez les prérequis administratifs à cette intrusion.
      i. Quels sont les risques encourus à bâcler cette étape ?
   b. Comment sont appelés les prestataires qui réalisent ces opérations d'audit?
      i. Par qui sont-ils habilités ?
      ii. Quelles sont les autres missions de cet organisme réalisant ces habilitations?
2. Eléments informatiques (2 points)
   a. Indiquez en cinq lignes maximum, comment prévoir une attaque via le protocole BGP sur les AS.
   b. On évoque ici un *audit en boite noire*. Que cela signifie-t-il et quels sont les autres types d'audit ?

2. Méthodes d'intrusion (8 points)

a. Intrusion (4 points)
   En trois lignes maximum par élément, indiquez quatre méthodes permettant d'initier une intrusion sur le SI de l'entreprise *Target.Inc*. Une des méthodes, au moins ne se limitera pas aux seules attaques informatiques.
b. Focus BYOD / *Bring Your Own Device* (3 points)
   En cette époque post-confinement, le télétravail s'est largement développé dans l'entreprise. Chaque employé peut via son téléphone portable (Android+iOS) accéder aux ressources de l'entreprise via client VPN ou pas.
   Indiquez en six lignes maximum les nouvelles opportunités que cela ouvre pour votre mission.

3. Conception / Réalisation (9 points)

Vous êtes dans la place! Vous disposez désormais d'un moyen de vous connecter depuis votre poste d'audit externe à un poste Windows d'un des employés de l'entreprise.

a. Progiciel et architecture matérielle (2 points)
   Le poste Windows dispose du client lourd pour le logiciel de comptabilité *MaCompta*. Une recherche sur le site de l'éditeur indique :
   - *« Compilé avec usage de canaris »*
   - *« Prise en compte des extensions NX sur les systèmes en disposant »*

   i. Expliquez ces deux indications et en quoi cela va impacter votre action.
b. Latéralisation et Elévation de privilèges (3 points)
   i. Décrivez chacun de ces deux principes.
c. Discrétion (2 points)
   i. Lors de cette attaque, vous souhaitez rester silencieux sur le SI. Identifiez deux contre-mesures que le défenseur aurait pu instancier pour vous contrecarrer dans cette démarche.
   ii. A chaque contre-mesure proposez une stratégie d'évitement pour atteindre votre but.

Le contrat stipule que vous devez valider la tenue en charge du site web de l'entreprise en cas de DDOS.

d. DDOS (1 point)
   Définissez et expliquez succinctement le principe d'un déni de service.
e. DDOS/Contremesure (1,5 point)
   Quelle(s) contre-mesure(s) l'entreprise pourrait avoir déployé pour garantir le service ?

4. Divers (3 points)

a. Stéganographie (1,5 points)
   Qu'est-ce que la stéganographie ? (En trois lignes maximum)
b. Mise en œuvre (1,5 points)
   Pouvez-vous en donner un exemple d'usage courant?

5. Hors Barème (+ 3 points supplémentaires)

a. Quel exemple d'usage stéganographique dans ce document et quelle en est la réponse ?

--

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Copie ayant obtenu la meilleure note

Spécialité : sciences et technologie - informatique

L'administration n'a volontairement pas corrigé les imperfections de fond et de forme dans les copies communiquées ci-après.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Année : 2021

Concours : Concours externe pour l'accès au corps des attachés

Épreuve : Spécialité Informatique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

Volet Blue Team.

1) Sécurité organisationnelle

1_1_a) L'acronyme OIV signifie Opérateur d'Importance Vitale. Il regroupe les acteurs jouant un rôle majeur dans les secteurs critiques pour la France (ex : Telecom, transport, gestion de l'eau). La notion d'OIV et les contraintes légales en matière de cybersécurité qui leur sont applicables sont définies par la loi de Programmation Militaire (LPM).

1_1_b) Les obligations légales liées à la qualification d'OIV sont les suivantes : Cartographie des Systèmes d'Information d'Importance Vitale (SIIV) et homologation de sécurité de ces systèmes par rapport au référentiel de la LPM. Ce référentiel définit par exemple des exigences en matière de cloisonnement / filtrage, d'administration et de journalisation.

c) L'Agence Nationale de Sécurité des SI (ANSSI) contrôle la conformité des OIV à la LPM en s'appuyant sur des prestataires d'audit certifiés (dits PASSI LPM).

1_2_a) Le recours à la prestation de service expose au risque de fuite de données suite à la compromission du prestataire, ainsi qu'à la compromission du SI du client à travers le SI du prestataire.

1-2-6- Contremesures aux risques ... cités supra :

* établissement d'un Plan d'Assurance Sécurité engageant le Prestataire sur des exigences sécurité (ex : sécurité physique, protection des données ...). Ce PAS sera un préalable à toute externalisation de données (ex : services d'hébergement).

* audits de sécurité du Prestataire, pour vérifier la bonne application du PAS ou des bonnes pratiques (par exemple par rapport à la norme ISO 27001), voire test d'intrusion si autorisé.

2) Sécurité Internet.

a) Cryptographie

i-1) le s de HTTPS signifie que la communication est chiffrée de bout-en-bout et que le serveur est authentifié par un certificat valide.

i-2) Le protocole utilisé est TLS (Transport Layer Security), qui offre chiffrement et authentification (serveur ou client + serveur) de la connexion. Durant le Handshake TLS, une clé symétrique est négociée via le protocole Diffie-Hellman, des ciphersuites sont élues entre client et serveur, et le client vérifie l'authenticité et la validité du certificat serveur.

i-3) La dernière version de TLS est TLS 1.3. Cette version offre le support des ciphersuites à l'état de l'art et garantit la propriété de Perfect Forward Secrecy (optionnelle en TLS 1.2). C'est surtout une garantie par rapport à un mauvais paramétrage de TLS 1.2, qui reste utilisable.

i-4) Sur les versions antérieures de ce protocole (SSL v.X), on peut citer les vulnérabilités POODLE ou HEARTBLEED. De façon générale, ce protocole est vulnérable à la compromission de l'autorité de certification, qui permet des attaques de l'homme du milieu.

ii - Il s'agit du Référentiel Général de Sécurité (RGS), défini et maintenu par l'ANSSI.

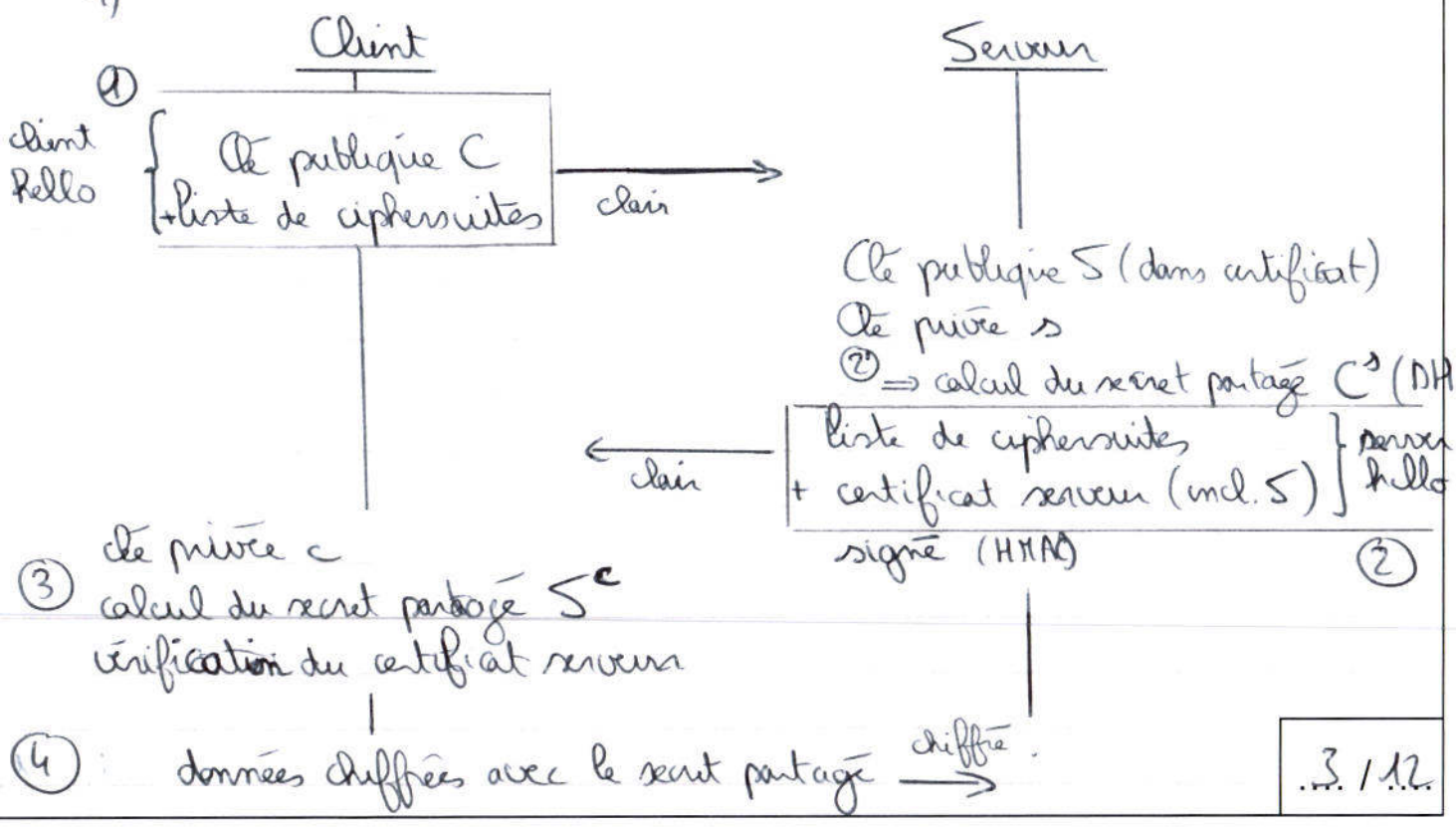
iii 1) Attributs du certificat serveur :
- Common Name (CN) : c'est l'identité du serveur (souvent son FQDN ou son Hostname)
- Date d'expiration : la date à partir de laquelle le client doit rejeter le certificat (à renouveler par le serveur).
- Issuer : c'est le nom de l'autorité de certification (AC) qui a délivré, c'est-à-dire signé, le certificat.

iii 2) L'autorité de certification ~~n'est~~ écroquée en 1) peut elle-même être certifiée par une autorité dite "parente" ; et ainsi de suite jusqu'à une autorité dite "racine". L'ensemble des certificats depuis l'autorité racine jusqu'à celle qui délivre le certificat serveur est la chaîne de certification.

iii 3) "Certificate invalid", parce que le certificat est expiré, ou révoqué, ou parce que l'autorité de certification est inconnue*. Une alerte empêchant tout accès au site est également possible, si celui-ci utilise le mécanisme HSTS.

* du navigateur.

4)



b) Développement

i) SQL (Structured Query language) est le langage algébrique utilisé pour l'interrogation de bases de données relationnelles.
Parfois, les requêtes du client sont insuffisamment validées par le serveur, ce qui permet à un client malveillant de faire exécuter par le serveur une requête SQL non autorisée. L'impact peut être la divulgation de l'ensemble de la base de données.

exemple : injection de la chaîne 'OR 1=1' dans l'URL, qui sera interprétée côté serveur comme SELECT X WHERE ... OR 1=1, qui est vraie pour toutes les relations.

ii) L'utilisation de strcpy expose à une vulnérabilité de type buffer overflow (débordement de mémoire tampon).

iii) segmentation fault (puisque l'on déborde de la zone mémoire allouée au processus). le système d'exploitation arrête l'exécution.

iv) Il faut valider la chaîne argv[1] avant de la passer à la fonction auth().
Soit ligne 12 : if (argc > 1 and len(argv[1]) < 33)
puisqu'on utilise un buffer de taille 32.

Année : 2021

Concours : Concours externe pour l'accès au corps des attachés

Épreuve : Spécialité Informatique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

3) Sécurité Intranet.

a) i) Le niveau fonctionnel d'un Active Directory est la version de son schéma, exprimée comme les versions de Windows Server (ex: 2012, 2012 R2, 2016...). Elle correspond aux attributs supportés. Par exemple, certains attributs POSIX utiles à l'intégration des systèmes UNIX dans l'AD nécessitent une montée de schéma.

ii) Etendre le schéma permet de s'affranchir des contraintes liées à une montée de version complète de l'infrastructure AD.

b) Mesure 1 - Mise en place d'un contrôle d'accès logique basé sur le standard 802.1x. Réduit le risque d'accès non autorisé au LAN par un terminal malveillant (ou non conforme).

Mesure 2 - Segmentation à l'aide de VLANs. Permet de limiter le risque de propagation sur le LAN à partir d'un terminal compromis (ex: passage de la bureautique au réseau de vidéosurveillance)

Mesure 3 : durcissement des commutateurs de desserte : changement du mot de passe par défaut, raccordement TACACS+ si disponible, etc. Permet d'éviter la compromission de l'infrastructure de desserte.

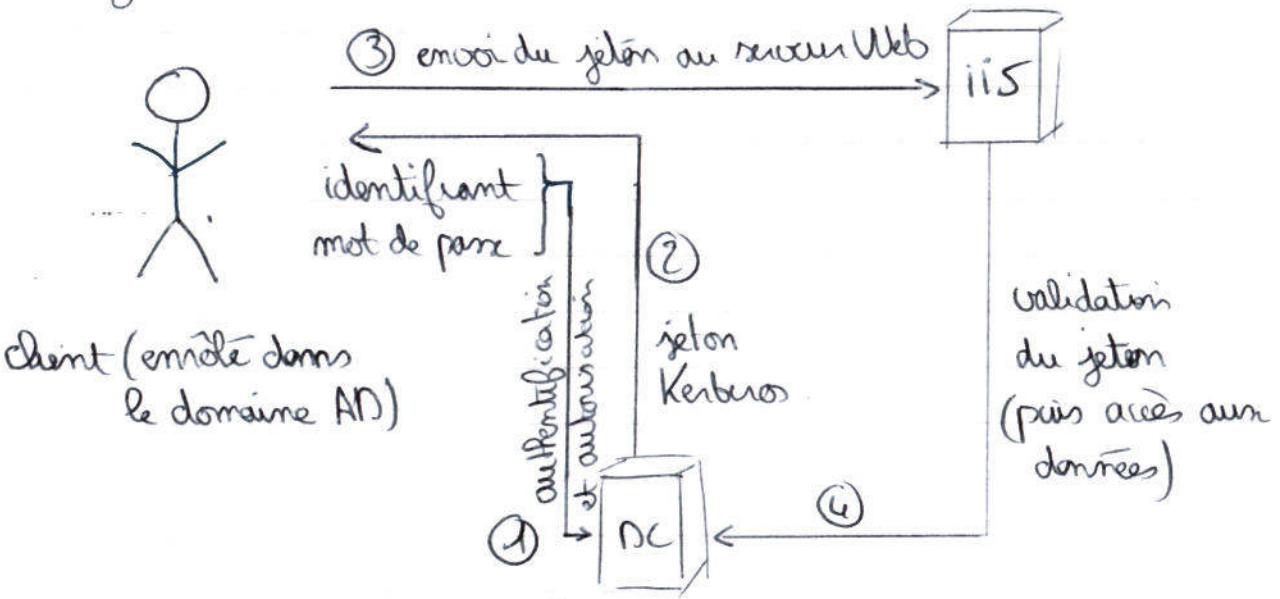
c) i) Windows 10 introduit notamment la technologie BitLocker, qui permet le chiffrement du disque sans ~~intervention~~ logiciel Tiers.
Il améliore également la gestion des secrets de l'utilisateur, en renforçant les API's et les mécanismes de stockage - notamment pour les secrets stockés par les navigateurs.

c_ii_1) Mesure 1 : raccordement via rsyslog à un système centralisé de gestion des traces (SIEM si possible).
Mesure 2 : authentification SSH par clés uniquement et autre durcissement de sshd.conf (ex : interdiction de se connecter en root).
Mesure 3 : création de comptes utilisateurs et services dédiés à chaque usage, avec contrôles fins des permissions root grâce au fichier sudoers.
Mesure 4 : activation de SELinux (attention, risque d'effet de bord).
Mesure 5 : raccordement à un annuaire centralisé pour l'authentification et l'autorisation, voire intégration à l'AD (ex : via sssd) pour faciliter la gestion du parc (mais attention au choix de l'AD vu le périmètre)
Mesure 6 : scans de vulnérabilité boîte noire et blanche réguliers et patching* en conséquence. *mise à jour

Mesure	Gain sécurité	Complexité.
1	Renforcée	+
2	Intermédiaire	- -
3	Elevé	-
4	Intermédiaire	+ +
5	Minimal	-
6	Elevé	+

d)i) Étant donné qu'il s'agit d'un serveur web IIS dans un environnement Active Directory, il est intéressant de privilégier les mécanismes Microsoft : un SSO utilisant le protocole Kerberos pour les utilisateurs titulaires de postes de travail managés, et une solution reposant sur la fédération d'identité Microsoft pour les tiers.

ii) Échange protocolaire



4) Infrastructure. (virtualisation)

En tant qu'OIV, Eaupuredotcom doit transformer son SI d'administration. Cela passe notamment par la séparation des tâches d'administration des SIIV et de bureautique pour ses équipes informatiques opérationnelles.
Après avoir étudié plusieurs pistes, c'est celle de la virtualisation qui est retenue : chaque administrateur disposera d'une machine virtuelle (VM) pour chaque type de tâche, accessibles depuis un terminal léger.
La solution CITRIX Xendesktop, pour laquelle des licences ont déjà été acquises, est retenue pour l'interface utilisateur. Elle s'appuie sur une infrastructure hyperconvergée NUTANIX (Dell) dimensionnée pour l'accueil des 100 administrateurs (croissance estimée à horizon 2025).
Compte-tenu du budget déjà conséquent engagé pour la conformité LPM, le même socle sera utilisé pour les postes bureautiques et d'administration (postes VDI CITRIX). L'isolation sera uniquement logique, ce qui permettra de fournir une redondance actif-actif sur nos deux sites.
L'intégration de la solution sera confiée à la société X, l'expertise en interne étant limitée et X ayant de bonnes références sur un projet similaire.
Le passage d'un seul poste de travail à ce nouvel environnement

(TSVP)

représentant un changement considérable pour nos administrateurs, une communauté Teams de support sera active pendant toute la durée du projet ~~et il sera précédé à une phase~~, qui sera précédé d'une phase pilote de 3 mois.

Volet Red Team

1) Préalable

1.1.a+i) Les prérequis administratifs à l'intrusion, habituellement consignés dans une lettre de mission à valeur contractuelle, sont les suivants :

- périmètre : quels sont les cibles à atteindre ? sur quelles périodes ?
- moyens : quelle est la durée de la prestation ~~et~~, le nombre d'auditeurs alloués et éventuellement leur outillage ?
- risques : quel impact le client est-il prêt à accepter (durée d'interruption du service, perte de données) ? Ce prérequis peut être chiffré en euros.

Faute d'une définition précise de ces modalités d'engagement, la prestation peut au mieux être inadaptée aux besoins du client, au pire endommager ses systèmes et entraîner une procédure légale à l'encontre du prestataire.

Année : 2021

Concours : Concours externe pour l'accès au corps des attachés

Épreuve : Spécialité : Informatique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

Volet Red Team - Préalable (suite)

1-b) les prestataires d'audit certifiés sont appelés Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI).

b) i) L'ANSSI certifie les auditeurs PASSI ainsi que leurs employeurs, via des tests individuels et l'audit du SMSI (Système de Management de la Sécurité Informatique).

ii) En complément, l'ANSSI assure la détection et la réaction aux incidents de sécurité affectant les SI de l'État et des OIV, par l'action du CERT-FR.

Elle qualifie et certifie également des solutions de sécurité ou d'hébergement (SecNumCloud), ainsi que les prestataires de réponse à incident (PRIS).

Enfin, elle définit le cadre réglementaire national en matière de SSI, incarné notamment par le RGS évoqué plus haut, et audite la conformité des opérateurs de télécommunications aux lois en vigueur.

2) a) Une attaque sévère mais difficile à mettre en œuvre sur le protocole BGP est le BGP-Hijacking. Elle consiste à annoncer sur le réseau de l'attaquant les préfix-lists correspondant à la victime, et ainsi aspirer son trafic.

Si la victime ne peut pas prévoir cette attaque et difficilement s'en prémunir, elle peut en détecter les prémices en constatant une baisse progressive du trafic vers son réseau.

2)b) Un audit boîte noire se fait sans accès ni connaissance préalable sur la cible. En boîte grise, l'auditeur dispose d'un accès à faibles privilèges, en blanche d'un accès à hauts privilèges.

2) Méthodes d'intrusion

2a) Méthode 1 : social engineering (ingénierie sociale) : appeler le support informatique Target Inc. en se faisant passer pour M. Portails et demander en urgence la réinitialisation de son mot de passe.
Méthode 2 : attaque Web : par injection SQL sur le site web www.targetinc.com, extraction de la base de donnée des clients de l'entreprise (grands groupes).
Méthode 3 : vol de poste de travail : sur le site de l'un des clients de Target Inc. (le plus vulnérable), dérober le poste de travail d'un salarié de Target Inc. et en extraire les données (s'il n'est pas chiffré).
Méthode 4 : typosquatting : achete le nom de domaine targetInc.com + BGP hijacking : aspirer le trafic à destination de l'AS 1982 et le rediriger vers targetInc.com pour dérober les identifiants des clients.

2_b) La première opportunité se situe au niveau de la passerelle VPN de l'entreprise, qui peut être mal configurée ou présenter une faille logicielle (car non patchée). Le client VPN étant optionnel, des services Web (exc : messagerie) sont également exposés à Internet, avec les mêmes risques. Enfin, le vol ou la compromission du téléphone peuvent respectivement ouvrir l'accès aux données ou au SI de Target Inc.

3) Conception / réalisation

a)

b) i) Latéralisation de privilèges : capacité à se déplacer d'un système à un autre avec des privilèges (utilisateur, administrateur...) de même niveau.

Elévation de privilèges : capacité à acquérir des droits plus élevés (ex : passer root depuis un compte Linux standard) sur un même système. L'utilisation de sudo est un exemple d'élévation de privilèges sur Linux.

c) Contremesure 1 : installation d'un agent dit EDR (Endpoint Détection and Response) sur le parc Windows. Cet agent a - au moins en théorie - la capacité de détecter et d'alerter sur les méthodes classique d'escalade.

Stratégie d'évitement 1 : aucune si on en croit les éditeurs ! Mais il reste possible de compromettre la console EDR si elle est mal durcie.

Contremesure 2 : export des journaux d'événements Windows vers un SIEM : plus manuelle et incomplète qu'un EDR, cette mesure sera plus utile en forensic qu'en détection de l'attaque.

d) Le déni de service est l'incapacité d'un service à traiter les requêtes qui lui sont adressées. Une attaque par déni de service (DOS), le plus souvent distribuée (DDOS), consiste à épuiser les ressources de la cible (CPU, table de session ... etc) pour provoquer un déni de service. On distingue les DDOS applicatifs et volumiques.

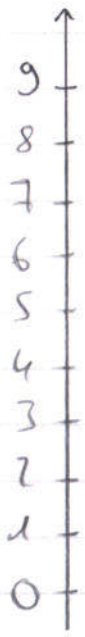
e) Les contremesures peuvent être de deux ordres : au niveau de serveurs Web par l'application d'un rate-limiting (par exemple à l'aide d'iptables), ou en amont de celui-ci au moyen d'une solution anti-ddos. Cette solution peut être interne (ex : batiers Arbor) ou déléguée à un tiers. Dans les deux cas, le trafic indésirable sera rejeté ou redirigé vers un "trou noir" (on parle de blackholing).

4) Steganographie.

a) La steganographie désigne l'ensemble de techniques permettant de dissimuler une donnée dans une autre (par exemple une image dans une autre image), sans recourir aux méthodes cryptographiques.

b) ..... le watermarking est un usage typique de la steganographie. Utilisé notamment par les ayants-droits de contenus vidéo, il permet d'incruster dans l'image des informations permettant d'identifier sa source en cas de piratage. Cette technique peut aussi permettre d'identifier où a été imprimé un document confidentiel, par exemple.

c) le barème ?



12.1/12