

Concours n°2019-AI-CE-03
Epreuve écrite du 28 juin 2019

Coefficient 2

A. Connaissances générales (8 questions à 0.5 pt)

1) Que signifie Ifsttar ?

2) A quel(s) Ministère(s) de tutelle est rattaché l'Ifsttar ?

- a) Ministère de la Transition écologique et solidaire
- b) Ministère de la cohésion des territoires
- c) Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation
- d) Ministère de l'Éducation nationale
- e) Ministère de l'Économie et des finances

3) RGPD signifie [0.5 pt]

- a) Réseau Gratuit et Privé de Données.
- b) Réseau Général pour la Protection des Données.
- c) Règlement Général et Public des Datacenters.
- d) Règlement Général pour la Protection des Données.

4) A quelle catégorie de la fonction publique appartient le corps des assistants ingénieurs (AI) ?

- a) A
- b) B
- c) C
- d) D

5) A quelle branche d'activité professionnelle appartient le poste auquel vous postulez ?

- a) C
- b) A
- c) F
- d) E

6) Quelle est la durée du stage avant titularisation d'une personne embauchée à l'Ifsttar?

- a) 3 mois
- b) 6 mois
- c) 12 mois
- d) 24 mois

7) Combien d'ETP compte l'Ifsttar ?

- a) 30
- b) 770
- c) 1050
- d) 250

8) L'Ifsttar n'est pas implantée à

- a) Belfort
- b) Bron
- c) Toulouse
- d) Marseille

B. Questions techniques (40 questions à 0,5 pt, parfois plusieurs réponses possibles)

1) Lequel de ces logiciels permet la création de machines virtuelles sur une machine exécutant Windows Server 2016 ?

- a) KVM
- b) Hyper-V
- c) DFS
- d) LVM

2) Quel protocole permet nativement la connexion à distance à une machine sous Windows Server 2016 ?

- a) SSH
- b) NetBIOS
- c) RDP
- d) HTTP

3) Quel organisme gère attribution des noms de domaine sur Internet ?

- a) L'ICANN
- b) L'OCDE
- c) RENATER
- d) L'ONU

4) Que signifie l'acronyme PRA ?

- a) panne de réplication de l'annuaire
- b) plan de reprise d'activité
- c) protection antivirale renforcée
- d) perte réseau asynchrone

5) La virtualisation ne permet pas

- a) la diminution de la consommation d'énergie
- b) de réduire le nombre de machine physique
- c) d'améliorer la sécurité
- d) d'optimiser l'utilisation de ressources matérielles.

6) laquelle de ces propositions n'est pas une solution de stockage dans le cloud ?

- 1) Nextcloud
- 2) Onedrive
- 3) Dropbox
- 4) Freebox

7) quel est le protocole par défaut utilisé par active directory ?

- a) SNMP
- b) Wrap
- c) LDAP
- d) Netbios

8) VHD est

- a) un conteneur de certificat Windows
- b) un disque dur virtuel
- c) une technologie réseau haut débit

d) un volume à haute densité de données

9) Quel est le type de mémoire des disques SSD ?

- a) morte
- b) vive
- c) volatile
- d) flash

10) N'est pas un langage de programmation

- A. HTML
- B. Pascal
- C. PHP
- D. Julia

11) Que permet l'utilitaire tracert sous Windows ?

- a) d'auditer l'ouverture de fichiers
- b) de créer un certificat pour signer des scripts
- c) de déterminer l'itinéraire d'un paquet réseau vers sa destination
- E) un keylogger qui enregistre tout ce qui est tapé au clavier

12) VSS sous Windows permet

- a) de virtualiser un système de fichier
- b) de se connecter en ssh sur un serveur linux
- c) de sauvegarder des bases de données
- d) de changer les ACL d'un dossier

13) L'ANSSI fait des recommandations sur les postes d'administration. Quelles préconisations sont fausses ?

- a) utiliser un équipement type "BYOD"
- b) protéger physiquement son poste
- c) utiliser un poste d'administration physiquement distinct de son poste d'usage bureautique.
- d) bloquer l'accès à internet sur le poste d'administration

14) Lequel de ces programmes ne permet pas l'archivage de fichiers ?

- a) 7zip
- b) Tar
- c) Winrar
- d) Winscp

15) Quels sont les rôles FSMO corrects ?

- a) Maître de schéma
- b) Maître des clés
- c). Maître d'infrastructure
- d). Maître de sécurité

16) Un hyperviseur bare-metal ?

- a) a besoin d'un système hôte
- b) a un accès direct au matériel
- c) permet la virtualisation
- d) n'est pas recyclable

17) Une adresse Mac est composée de

- a) 6 octets
- b) 16 bits
- c) 12 octets
- d) 12 bits

18) KMS est

- a) un ver
- b) un système d'activation de licence Microsoft
- c) un langage de programmation
- d) une distribution Linux

19) Quel outil permet de manipuler la base de registre Windows ?

- a) regedit.exe
- b) registry.exe
- c) reg.exe
- d) openreg.exe

20) Que signifie l'acronyme LDAP ?

- a) Lightweight Direction Autorisation Protocol
- b) Local Directory Access Priority
- c) Lightweight Directory Access Protocol
- d) Low Direction authentical Program

21) WSUS

- a) permet une connexion sécurisée à un réseau Wifi
- b) propose des mises à jour système et logicielle à un système Windows
- c) permet d'overclocker le GPU de sa carte graphique
- d) permet la suppression de malwares

22) quelle est la date de fin de support de Windows 7 ?

- a) 14 janvier 2020
- b) 11 novembre 2019
- c) 15 janvier 2021
- d) 24 octobre 2020

23) Que signifie SQL ?

- a) Structured Query Language
- b) Structured Question Langage
- c) Stream Question Langage
- d) Strong Query Langage

24) Quel résultat donne les lignes powershell suivantes ?

`$os="windows"`

`Write-host $os,"$os",'$os'`

- a) une erreur
- b) windows, windows, windows
- c) windows windows \$os
- d) windows "windows" windows

25) Quel est la commande qui permet de récupérer son adresse mac sous Windows ?

- a) ping localhost
- b) ipconfig /all
- c) ipconf

d) ifconfig

26) Quel est le protocole d'authentification principale de Windows ?

- a) LDAP
- b) Kerberos
- c) Radius
- d) Chap

27) Que signifie l'acronyme SAN ?

- a) Storage Administration Network
- b) Security Administration Network
- c) Storage Area network
- d) Structure Area network

28) Le protocole LDAP permet :

- a) de tester la sécurité du SI
- b) d'administrer un annuaire
- c) d'archiver les données des utilisateurs
- d) de démarrer un poste à distance

29) Un serveur DNS permet

- a) de traduire un nom de domaine internet en adresse IP
- b) de geolocaliser un ordinateur
- c) de configurer la carte réseau d'un ordinateur
- d) de sécuriser la navigation sur internet

30) Que signifie l'acronyme RAID ?

- a) Récupération Aléatoire Incident Disque
- b) Redundant Array of Independent Disks
- c) Réseau Informatique Aérien Dématérialisé
- d) Return Access Inodes Disks

31) Sous Windows quelle est la commande ou l'outil qui permet de lister les processus ?

- a) ps
- b) get-process
- c) sc
- d) tasklist

32) Quel est le port utilisé par le service nommé « Netbios Session Service » ?

- a) 21
- b) 137
- c) 139
- d) 25

33) Que fait cette commande, robocopy d:\travail z:\mon-espace /mir ?

- a) copie le dossier d:\ travail vers z:\mon-espace\travail
- b) synchronise le dossier d:\travail avec le dossier z:\mon-espace
- c) copie le dossier d:\travail vers z:\mon-espace en ignorant les dossiers vides
- d) restore le dossier d:\travail depuis le dossier z:\mon-espace

34) La mémoire swap est ?

- a) de la mémoire supplémentaire disponible en ROM
- b) la mémoire principale de l'ordinateur

- c) une extension de la mémoire vive sur la mémoire de masse
- d) une barrette mémoire défectueuse

35) Que signifie l'acronyme DHCP ?

- a) Dynamic Host Configuration Protocol
- b) Dynamic Host Control Protocol
- c) Dynamic Hot Current protocol
- d) Dynamic hook correction protocol

36) L'activation de VSphere HA sur un cluster permet ?

- a) d'accélérer le chargement des applications
- b) de redémarrer les VM d'un nœud qui ne répond plus sur les autres membres du cluster
- c) la continuité de service sans aucune interruption
- d) d'éteindre simultanément toutes les VM du cluster

37) Que fait la commande powershell suivante ?

(Invoke-WebRequest -Uri "https://www.ifsttar.fr/accueil/").Links.Href

- a) Elle télécharge la page d'accueil du site web de l'Ifsttar sur votre poste
- b) Elle cherche les liens morts sur la page d'accueil du site web de l'Ifsttar
- c) Elle affiche les liens de la page d'accueil du site web de l'Ifsttar
- d) Elle cherche des failles de sécurité sur la page d'accueil du site web de l'Ifsttar

38) Que signifie GPT ?

- a) Guid Partition Table
- b) Graph Program Temperature
- c) Global Provisioning Tools
- d) Ghost Process Terminated

39) Pour protéger votre vie privée vous faites confiance ?

- a) à la CNIL
- b) à la CNAV
- c) à Facebook
- d) à votre firewall

40) La blockchain est une technologie

- a) qui permet de bloquer une attaque de virus
- b) sécurisée de stockage et de transport d'information
- c) de déploiement logiciels par paquets MSI
- d) qui va remplacer le Bios

C. QUESTIONS OUVERTES

1) Quels sont les principaux services rendus par un Active Directory ? Que représente dans ce contexte la notion d'Organizational Unit (OU) ? Quels usages et avantages peut-on avoir dans l'utilisation de ces OU ? [2 pts]

2) Dans l'exploitation quotidienne d'un Active Directory on évoque souvent les GPO. En quoi sont-elles utiles dans une gestion de parc informatique ? Expliquez brièvement leur mise en œuvre (création / exécution d'une GPO). [2 pts]

3) Quels sont les différents composants d'une infrastructure Skype Entreprise « on premise » ? Placez-les sur un schéma réseau et expliquez leur rôle. [3 pts]

4) Votre établissement souhaite donner accès aux données et applications à ses utilisateurs nomades ou travaillant à domicile. Quel dispositif mettez-vous en place ? Décrire son fonctionnement, les outils nécessaires, les avantages et les inconvénients. [3 pts]

D. Compréhension d'un texte en anglais (cf Document en Annexe 1)

Quelle est l'idée générale du document ? [1 pts]

Décrivez le mode de fonctionnement de la vulnérabilité [2 pts]

Quel est le risque encouru et ses conséquences ? [1 pts]

Quelle solution mettez-vous en œuvre ? [2 pts]

ANNEXE 1

1.1 CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

1.1.1 Security Vulnerability

Published: 05/14/2019

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

1.2 Mitigations

The following mitigation may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave Remote Desktop Services disabled:

1. Disable Remote Desktop Services if they are not required.

If you no longer need these services on your system, consider disabling them as a security best practice. Disabling unused and unneeded services helps reduce your exposure to security vulnerabilities.

1.3 Workarounds

The following workarounds may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave these workarounds in place:

1. Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2

You can enable Network Level Authentication to block unauthenticated attackers from exploiting this vulnerability. With NLA turned on, an attacker would first need to authenticate to Remote Desktop Services using a valid account on the target system before the attacker could exploit the vulnerability.

2. Block TCP port 3389 at the enterprise perimeter firewall

TCP port 3389 is used to initiate a connection with the affected component. Blocking this port at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks. However, systems could still be vulnerable to attacks from within their enterprise perimeter.

1.4 Acknowledgements

The UK's National Cyber Security Centre (NCSC)

1.5 Disclaimer

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

1.6 Revisions

Version	Date	Description
1.0	05/14/2019	Information published.

1.6.1.1