

Concours externe de Assistant ingénieur
BAP : E (Informatique, statistique et calcul scientifique)
Emploi-type : Gestionnaire de parc informatique et télécommunications

Nom :
Nom de jeune fille :

Prénom :

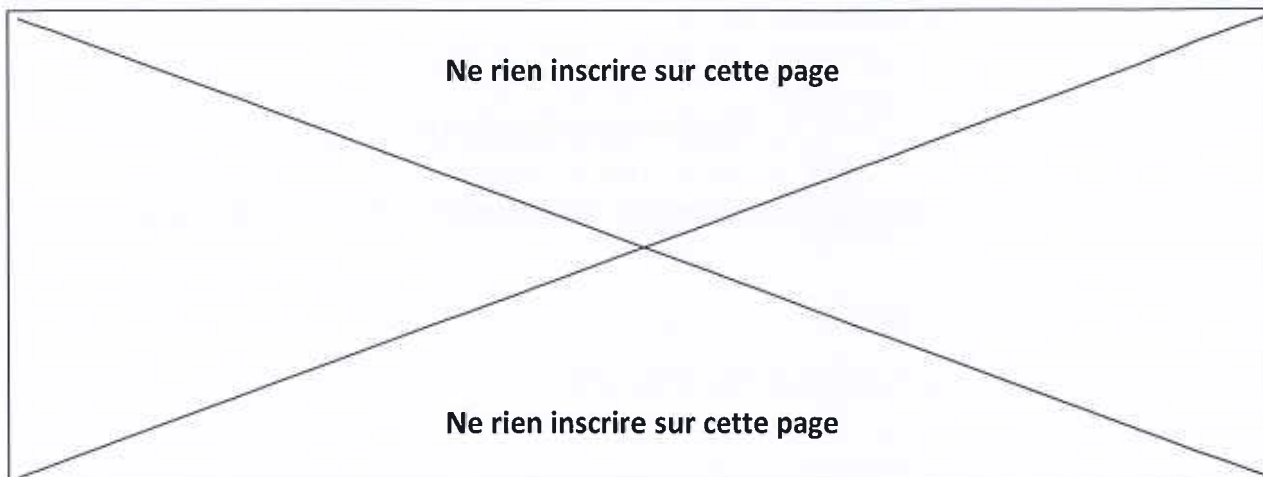
Date de naissance :



Note : /20

Epreuve d'admissibilité – Durée : 3h – Coefficient : 4

Vendredi 17 juin 2016 de 14h à 17h



Instructions

Ce sujet comporte **30 pages**

Assurez-vous que cet exemplaire soit complet. S'il est incomplet, demandez un nouvel exemplaire au surveillant de salle.

Il vous est rappelé que votre identité ne doit figurer que sur la première page de la copie. Toute mention d'identité portée sur toute ou partie de la copie que vous remettrez en fin d'épreuve mènera à l'annulation de votre épreuve.

Ne sont pas autorisés dans la salle d'examen

- Les téléphones mobiles et PDA
- Les agendas, journaux, revues etc...
- Dictionnaires, encyclopédies et ouvrages de référence.
- Tout type d'ordinateur personnel et de calculatrice.

NE PAS ECRIRE AU CRAYON À PAPIER SUR LA COPIE D'EXAMEN

Vous répondrez directement sur le sujet.

Vous reporterez les réponses du QCM sur la grille de saisie des réponses jointe au sujet.

NOM PATRONYMIQUE :

NOM MARITAL :

PRENOM(S) :

Notation et décompte des points :

Nombre de points maximum : 100 points (ramenés à une note sur 20)

Section 1 (25 points)

Section 2 (35 points)

Section 3 (16 points)

Section 4 (16 points)

Section 5 (8 points)

Organisation du sujet :

- 1 - QCM : 45 questions
- 2- Etude de cas, mise en situation
- 3 - Gestion de projets - étude de besoin
- 4 – Organisation d'un service support aux usagers
- 5 - Compréhension d'un texte en anglais avec questions en français, réponses en français

1 - QCM : 45 questions – 25 pts – une seule réponse par question

Veillez remplir au stylo noir les cases retenues pour votre réponse et veillez à ne faire apparaître aucune écriture dans les cases non retenues, comme indiqué sur la fiche ci-joint. Vous disposez d'une ligne « repentir » pour chaque question qui vous permet de revenir sur votre choix initial pour faire une nouvelle proposition.

Toute ambiguïté entraînera un décompte NUL (0 point) pour l'affirmation.

1 – Que signifie PRA ?

- A. Adresse Réseau Privée
- B. Plan Reprise Activité
- C. Private Relation Administrator
- D. Plan Réseau Adresses
- E. Prime Recherche ASI

2 – Quelle est le meilleur mot de passe ?

- A. 123Soleil
- B. Password
- C. \$tRj45*fdC
- D. %rtAmmAtr%
- E. Alexandra*%

3 – Laquelle de ces méthodes n'est pas une méthode Agile ?

- A. eXtreme Programming
- B. Scrum
- C. Kanban
- D. RAD
- E. MVC

4 – Quelle proposition n'est pas un CMS ?

- A. Drupal
- B. Joomla
- C. WordPress
- D. Symfony
- E. SPIP

5 – Quel port est associé au protocole SMTP ?

- A. 443
- B. 80
- C. 25
- D. 22
- E. 21

6 – Quelle commande permet d'installer un logiciel sous Windows ?

- A. Apt-get
- B. Yum
- C. MsiExec
- D. Gcc
- E. Aptitude

7 – Parmi ces propositions, laquelle n'est pas un algorithme de chiffrement ?

- A. AES
- B. TAR
- C. 3DES
- D. Blowfish
- E. DES

8 – Laquelle de ces propositions n'est pas un SGBD ?

- A. Mysql
- B. Oracle
- C. MSSQL
- D. Bdd
- E. Postgres

9 – En base de données, qu'est ce qui permet d'identifier de façon unique un enregistrement dans une table ?

- A. Clé secondaire
- B. Clé primaire
- C. Attribut
- D. Clé étrangère
- E. Cardinalité

10 - Parmi ces technologies lequel permet de créer un VPN

- A. IPv4
- B. IPv6
- C. IPsec
- D. ICMP
- E. SDSL

11 - Laquelle de ces propositions n'est pas une solution de virtualisation

- A. Hyper V
- B. KVM
- C. VirtualBox
- D. VMWare
- E. DropBox

12 - A quoi servent les jointures dans une base de données ?

- A. À valider le schéma
- B. À relier les identifiants de même nom dans plusieurs tables
- C. À associer des identifiants identiques de même nature
- D. À faire un tri
- E. À valider une requête

13 - Dans la liste suivante, quelle base de données est issue du monde libre ?

- A. Access
- B. DB2
- C. Oracle
- D. SQL Server
- E. PostgreSQL

14 - Parmi ces logiciels lequel n'est pas un serveur d'application Java ?

- A. Geronimo
- B. Tomcat
- C. Weblogics
- D. WebObjects
- E. Apache

15 - Que définit l'enregistrement de type MX dans un serveur de nom DNS ?

- A. Un pointeur vers un serveur de messagerie
- B. Un pointeur vers un DNS secondaire
- C. Un alias vers un nom de domaine
- D. Un serveur de DIVX
- E. Un pointeur vers le nom du domaine principal

16 - Quel ordre SQL permet de modifier la structure d'une table de données :

- A. CREATE
- B. ALTER
- C. SELECT
- D. UPDATE
- E. DELETE

17 - Dans une base de données relationnelle, je souhaite sélectionner tous les enregistrements d'une table nommée "PRODUITS". Choisissez la requête SQL convenant

- A. Select distinct id from PRODUITS
- B. Select * from PRODUITS where reference not null
- C. Select * from PRODUITS
- D. Select * where PRODUITS
- E. Select all from PRODUITS

18 - Le PERT (Program of Evaluation and Review Technique) est

- A. Un langage de programmation
- B. Un outil d'évaluation de logiciels
- C. Un outil de « reverse ingenierring »
- D. Un protocole internet
- E. Un outil de planification

19 - L'instruction suivante en SQL « Select nom,count(*) from ville where nombre_habitants > 100000 group by nombre_habitants ; » permet :

- A. De lister les noms des villes de plus de 100 000 habitants
- B. D'avoir les noms de villes et leur nombre d'habitants
- C. D'avoir la liste des villes et leur nombre d'habitants pour les villes de plus de 100 000 habitants
- D. Avoir le nombre d'habitants par ville
- E. Ne fonctionne pas

20 - Quelle connectique est à la fois capable de transmettre des données, de la vidéo et du courant à plusieurs Gbit/s, tout en étant réversible ?

- A. HDMI
- B. DVI-A
- C. USB 3.1
- D. DVI-D
- E. USB – Type C

21 - Lequel de ces produits est un chargeur d'amorçage libre :

- A. CUP
- B. LILOU
- C. GRUB
- D. BLAG
- E. Config.sys

22- Comment s'appelle le navigateur natif de Windows10 :

- A. Netscape
- B. Edge
- C. Safari
- D. Chromium
- E. Konqueror

23 - Que signifie le sigle SGBD ?

- A. Système de Gestion de Base de Données
- B. Sauvegarde et Gestion de Base de Données
- C. Système de Gestion de Bandes Dessinées
- D. Son et Graphisme en Base de Données
- E. Sauvegarde du Glossaire des Biens Dématérialisés

24 -Que signifie le sigle MCD :

- A. Modèle Constitutif de Données
- B. Manage and Choose Data
- C. Minor Choice Decision
- D. Modèle Conceptuel de Données
- E. Modèle Consistant de Données

25 - L'instruction suivante en SQL : « SELECT nom FROM agent WHERE age>10 ORDER BY age ; » permet de :

- A. classer les agents par ordre alphabétique
- B. lister les agents par groupe de 10
- C. lister le nom de tous les agents de la table agent
- D. lister le nom des agents de plus de 10 ans classés par âge
- E. lister l'âge de tous les agents

26 - Quel est le protocole utilisé pour l'échange de clé dans l'établissement d'un tunnel VPN IPSEC

- A. HTTPS
- B. IKE
- C. X509
- D. SSH
- E. LDAPS

27 - Quel type de RAID n'est pas tolérant à la panne d'un disque ?

- A. RAID 1
- B. RAID 5
- C. RAID 50
- D. RAID 6
- E. RAID 0

28 - Quel est le masque de sous réseau par défaut d'un réseau de classe C

- A. 255.255.255.0
- B. 255.0.0.0
- C. 255.255.255.255
- D. 255.255.0.0
- E. 0.0.0.0

29 - Lequel de ces modèles n'est pas optimal pour l'organisation d'un service :

- A. BPMN
- B. ITSM
- C. ITIL V3
- D. ISO 20000
- E. CMMI-SVC

30 - La sécurité du système d'information repose sur 3 critères :

- A. Disponibilité - intégrité - Confidentialité
- B. Pérennité - confidentialité - sécurité
- C. Stabilité – intégrité - sécurité
- D. Identification - Protection - Restauration
- E. Traçabilité - incorruptibilité- Disponibilité

31 - Pour effectuer l'achat de 30 PC de votre parc lors d'un renouvellement vous devez :

- A. Acheter ce matériel chez votre fournisseur habituel
- B. Commander sur internet obligatoirement
- C. Respecter le code des marchés publics
- D. Chercher un fournisseur qui n'a pas de frais de port
- E. Commander en Chine car c'est moins cher

32 - Pour garantir une bande passante suffisante lors de visio-conférences dans un établissement vous devez :

- A. Appeler le FAI qui dessert l'établissement
- B. Mettre en place de la QoS pour cet établissement
- C. Demander aux utilisateurs de cet établissement de ne faire aucun autre usage d'internet pendant la durée de la visio
- D. Limiter le nombre de visio
- E. Mettre en place un boîtier anti-DDOS sur cet établissement

33 - Lorsque vous installez un poste de travail, vous ne devez pas :

- A. Recenser les licences de logiciels que vous installez dessus
- B. Répertorier le PC dans l'inventaire de votre établissement
- C. Vérifier si le poste rend bien les fonctionnalités attendues
- D. Le connecter au réseau de l'établissement
- E. Installer des logiciels dont l'établissement ne possède pas la licence

34 - Depuis quelle date Windows XP n'est plus supporté par Microsoft ?

- A. Avril 2014
- B. Janvier 2015
- C. Décembre 2015
- D. Février 2016
- E. Ce n'est pas encore le cas

35 - Le BYOD c'est :

- A. Le salarié qui connecte son matériel personnel au réseau de l'entreprise
- B. Le salarié qui utilise les PC de l'entreprise chez lui
- C. Un PC de l'entreprise utilisé en déplacements
- D. Buy your old device
- E. Quand il y a trop de casse de PC dans l'entreprise

36 - Pour que l'employeur n'ait pas le droit de visionner un répertoire du disque dur d'un employé il faut :

- A. Que l'employé ait fait un mail à son employeur indiquant où se trouvent les données personnelles
- B. Que le répertoire personnel soit avec un attribut caché
- C. Que celui-ci soit clairement identifié comme étant un répertoire « personnel » en le nommant ainsi
- D. Que l'administrateur du parc n'ait pas le droit de se connecter à la machine de l'employé
- E. Que l'employé ait crypté le répertoire personnel

37 - Quelle réponse ne correspond pas à un logiciel de déploiement d'image système

- A. FOG
- B. Imagedeploy
- C. SCCM
- D. Ghost
- E. Clonezilla

38 - Qu'appelle-t-on authentification forte ?

- A. Une combinaison d'au moins deux facteurs d'authentification
- B. Une authentification utilisant à minima un hash md5.
- C. Une authentification avec un mot de passe type passphrase, associée à une clé RSA 128bits.
- D. Une authentification aléatoire.
- E. Une authentification basée sur un Single Sign-On.

39 - Quel service faut-il désactiver sur un serveur pour éviter qu'il ne serve de relai de messagerie en cas de compromission :

- A. SMTP
- B. IMAP
- C. POP3
- D. SNMP
- E. SSH

40 - Parmi les commandes suivantes laquelle peut être utilisée sous Windows pour afficher la configuration ip actuelle du système :

- A. configip
- B. ipconfig
- C. ifconfig
- D. winconfig
- E. tracertip

41 - Le port d'un service réseau est 143. À quel service cela correspond-il ?

- A. FTP
- B. IMAP
- C. POP3
- D. SNMP
- E. DHCP

42 - Combien faut-il avoir de disque minimum pour avoir du RAID5

- A. 1 disque
- B. 2 disques
- C. 3 disques
- D. 4 disques
- E. 5 disques

43 - Qu'est-ce que le protocole HTTPS ?

- A. Le protocole HTTP en version multi-poste
- B. Une ancienne version du protocole HTTP
- C. La version sécurisée du protocole HTTP
- D. Un protocole d'accès aux vidéos numériques
- E. Un langage de description de page comme le format HTML

44 - Que signifie l'acronyme CNIL ?

- A. La Commission Nationale des Informations Libres
- B. La Caisse Nationale des Informaticiens Libéraux
- C. La Commission Nationale de l'Informatique et des Libertés
- D. La Communauté des Nouvelles Informations Libres
- E. La Commission Nationale d'Informatique Légale

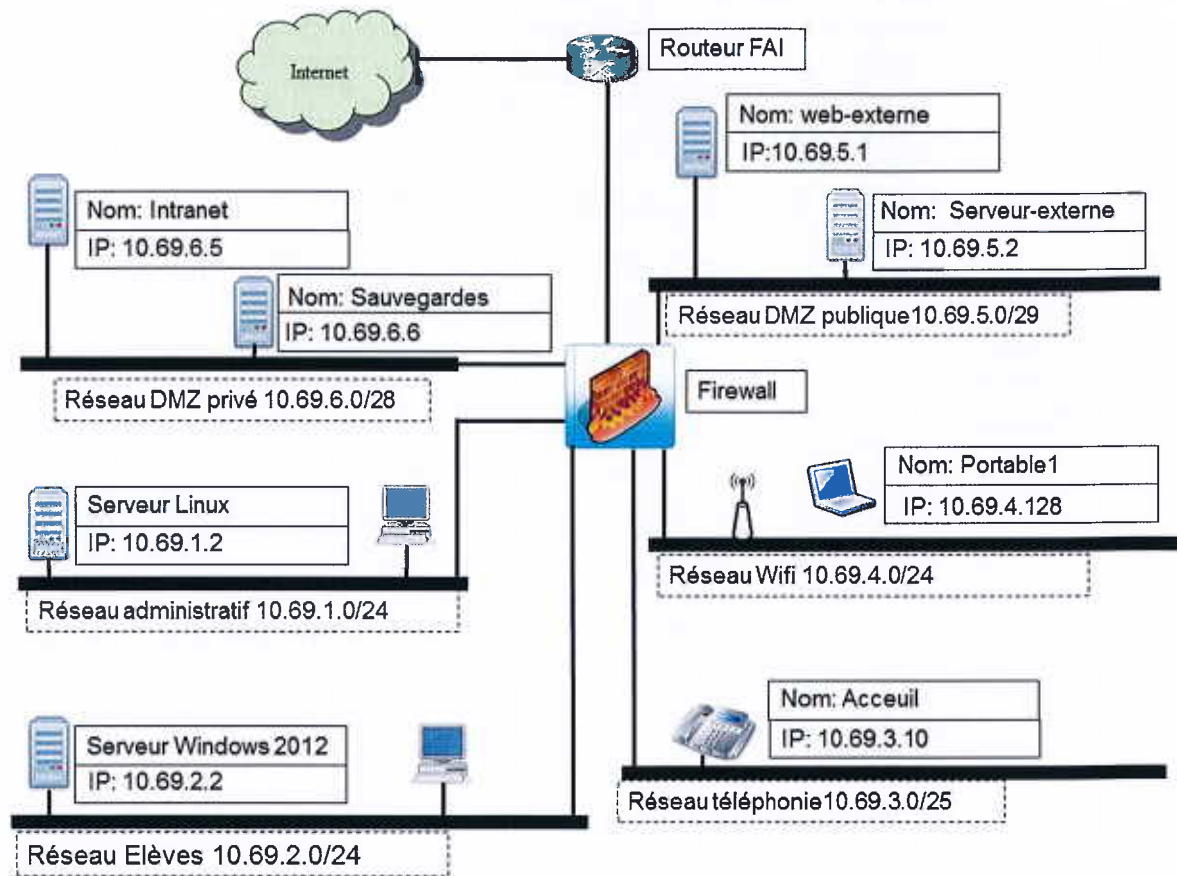
45 - Sachant qu'IPv4 utilise 32 bits d'adresses, le protocole IPv6 utilise :

- A. 16 bits
- B. 32 bits
- C. 64 bits
- D. 128 bits
- E. 256 bits

Questions Système/réseaux : 35 points

Il sera tenu compte dans la notation de l'orthographe et de la qualité de la rédaction

Le pare-feu est un serveur Linux sous Ubuntu qui possède 7 zones (7 cartes ethernet). Ce serveur assure en autres, le routage avancé et le filtrage d'adresses IP entre zones.



Système

Q1 : Serveur de nom DNS. Donnez l'application ou le service sous Linux qui gère ce service ?

Q2 : Service de Cache Web. Donnez l'application ou le service sous Linux qui gère ce service ?

Q3 : Authentification des utilisateurs par SSO. Expliquez ce qu'est SSO et donnez l'application ou le service sous Linux qui permet de gérer ce service ?

Q4 : Filtrage de site. Donnez l'application ou le service sous Linux qui gère ce service ?

--

Q5 : Le pare-feu fait également serveur DHCP. Expliquez ce qu'est un DHCP et combien faut-il gérer de zones différentes?

IPv4

Un bloc de 8 adresses IPv4 publiques 194.199.229.0 est réservé à la zone entre le routeur et le pare-feu.

Q6 : Donnez le masque de ce sous réseau ?

--

Q7: Combien d'adresses IP restent disponibles ?

--

Q8 : On souhaite que le réseau élèves puisse gérer 1090 postes ? Donnez le masque de sous réseau et le nombre de machines qu'il sera possible de mettre dans ce nouveau réseau.

Routage IP

Q9 : Donnez une commande pour afficher la table de routage sur le pare-feu Linux.

Q10 : Complétez la table de routage du pare-feu ci-dessous

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
194.199.229.0	0.0.0.0	_____._____	U	1	0	0	eth0
10.69.1.0	0.0.0.0	_____._____	U	1	0	0	eth1
10.69.2.0	0.0.0.0	_____._____	U	1	0	0	eth2
10.69.3.0	0.0.0.0	_____._____	U	1	0	0	eth3
10.69.4.0	0.0.0.0	_____._____	U	1	0	0	eth4
10.69.5.0	0.0.0.0	_____._____	U	1	0	0	eth5
10.69.6.0	0.0.0.0	_____._____	U	1	0	0	eth6
0.0.0.0	194.199.229.1	_____._____	____	0	0	0	eth0

Q11 : En déduire l'adresse interne du routeur (côté LAN).

Protocoles

Q12 : Quels ports doit-on ouvrir sur le pare-feu pour accéder au serveur Web placé sur la DMZ publique ?

Q13 : Quels ports doit-on ouvrir sur le pare-feu pour accéder au serveur de courrier qui fait également Webmail placé sur la DMZ publique ?

Q14 : Quels ports doit-on ouvrir sur le pare-feu pour accéder en toute sécurité à l'administration distante du pare-feu en mode commande ?

Wifi protocoles et radius

Q15 : Donnez les normes WIFI que vous connaissez et donnez en les principales caractéristiques.

Q16 : Quel est le protocole Wifi qui devrait être utilisé pour communiquer en toute sécurité avec une borne Wifi ?

Q17 : Quel est le standard d'authentification d'un serveur Radius et quels sont les protocoles d'authentification associés ?

Sauvegardes

Q18 : Quelle organisation vous pouvez proposer pour la sauvegarde des données utilisateurs présentes sur les serveurs Windows et Linux?

Q19 : Listez et expliquez les serveurs de stockage en réseau que vous connaissez ?

IPv6

Q20 : Donnez les trois types d'adresses IPv6

Q21 : Comment se fait l'auto configuration des postes dans un réseau avec IPv6. Cette auto configuration utilise quel protocole ?

Pare-feu Linux

Q22 : Expliquez la commande ci-dessous :

`iptables -A INPUT -p icmp -j DROP`

Q23 : De manière globale sur un firewall quelle devrait être la première règle ? La dernière règle ?

Scripts

Voici 2 scripts:

Script1: script.ps1

```
[CmdletBinding()]  
Param  
(  
    [Parameter(Mandatory=$true)][string] $drive,  
    [Parameter(Mandatory=$true)][string] $computer  
)  
  
$driveData = Get-WmiObject -class win32_LogicalDisk -computername $computer |  
?{$_.deviceID -like $drive + "*"}  
  
$fSpace = $driveData.FreeSpace/1024/1024/1024  
  
$fSpace = "{0:N2}" -f $fSpace  
  
Write-Host -foregroundcolor green "$fSpace Go on $drive."
```

Script2: script.sh

```
#!/bin/bash  
  
read part  
  
read computer  
  
fspace=`ssh $computer df -h | grep $part | awk '{print $4}'`  
  
echo "$fspace Go on $part"
```

Q24: Dans quel type d'environnement le **script1** est-il exécuté ?

--

Q25: Les deux scripts réalisent la même fonction, décrivez brièvement laquelle?

Cron :

Voici l'extrait de la commande `crontab -l` lancée sur le serveur de sauvegarde:

```
root@sauvegarde:~# crontab -l  
  
#sauvegardes  
  
21 23 * * 1-5 /root/scripts/journalier.sh  
21 23 * * 6 /root/scripts/full.sh  
  
#maj  
  
0/5 * * * * /root/scripts/verif_update.sh  
  
  
# hbty  
  
00 09 04 11* /root/script/hbty.sh
```

Q26: Quelle est la principale différence entre la commande « cron » et la commande « at » ?

Q27 : Donnez les fréquences d'exécution pour les différents scripts :

journalier.sh :

full.sh :

verif_update.sh :

hbty.sh :

TCPDUMP :

Q28 : En analysant le résultat de la commande suivante que pouvons-nous déduire ?

root@serveur2: **tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes**

16:59:26.680713 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [S], seq 2097828868, win 29200, options [mss 1380,sackOK,TS val 656141767 ecr 0,nop,wscale 7], length 0

16:59:26.680758 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [S.], seq 302911815, ack 2097828869, win 28960, options [mss 1460,sackOK,TS val 2570267615 ecr 656141767,nop,wscale 7], length 0

16:59:26.681140 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [.], ack 1, win 229, options [nop,nop,TS val 656141767 ecr 2570267615], length 0

16:59:26.682157 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 1:66, ack 1, win 227, options [nop,nop,TS val 2570267615 ecr 656141767], length 65

16:59:26.682415 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [.], ack 66, win 229, options [nop,nop,TS val 656141768 ecr 2570267615], length 0

16:59:26.682464 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 1:34, ack 66, win 229, options [nop,nop,TS val 656141768 ecr 2570267615], length 33

16:59:26.682471 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [.], ack 34, win 227, options [nop,nop,TS val 2570267615 ecr 656141768], length 0

16:59:26.682968 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 66:221, ack 34, win 227, options [nop,nop,TS val 2570267615 ecr 656141768], length 155

16:59:26.683329 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 34:44, ack 221, win 237, options [nop,nop,TS val 656141768 ecr 2570267615], length 10

16:59:26.683427 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 221:251, ack 44, win 227, options [nop,nop,TS val 2570267615 ecr 656141768], length 30

16:59:26.683993 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 44:298, ack 251, win 237, options [nop,nop,TS val 656141768 ecr 2570267615], length 254

16:59:26.689808 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 251:1433, ack 298, win 235, options [nop,nop,TS val 2570267617 ecr 656141768], length 1182

16:59:26.695049 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 298:424, ack 1433, win 260, options [nop,nop,TS val 656141771 ecr 2570267617], length 126

16:59:26.696114 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 1433:1659, ack 424, win 235, options [nop,nop,TS val 2570267619 ecr 656141771], length 226

16:59:26.696670 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 424:486, ack 1659, win 278, options [nop,nop,TS val 656141771 ecr 2570267619], length 62

16:59:26.696746 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 1659:1829, ack 486, win 235, options [nop,nop,TS val 2570267619 ecr 656141771], length 170

16:59:26.697115 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 486:615, ack 1829, win 297, options [nop,nop,TS val 656141771 ecr 2570267619], length 129

16:59:26.706239 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 1829:1923, ack 615, win 243, options [nop,nop,TS val 2570267621 ecr 656141771], length 94

16:59:26.706819 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 615:1053, ack 1923, win 297, options [nop,nop,TS val 656141774 ecr 2570267621], length 438

16:59:26.717633 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 1923:1986, ack 1053, win 252, options [nop,nop,TS val 2570267624 ecr 656141774], length 63

16:59:26.727088 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 1053:1088, ack 1986, win 297, options [nop,nop,TS val 656141779 ecr 2570267624], length 35

16:59:26.727102 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [P.], seq 1088:1119, ack 1986, win 297, options [nop,nop,TS val 656141779 ecr 2570267624], length 31

16:59:26.727108 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [F.], seq 1119, ack 1986, win 297, options [nop,nop,TS val 656141779 ecr 2570267624], length 0

16:59:26.727174 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [P.], seq 1986:2030, ack 1120, win 252, options [nop,nop,TS val 2570267626 ecr 656141779], length 44

16:59:26.727285 IP 10.69.5.2.25 > 10.69.4.128.45680: Flags [FP.], seq 2030:2061, ack 1120, win 252, options [nop,nop,TS val 2570267626 ecr 656141779], length 31

16:59:26.727440 IP 10.69.4.128.45680 > 10.69.5.2.25: Flags [R.], seq 2097829988, win 0, length 0

Commutateur

Q29 : À quoi correspond la norme IEEE 802.1Q ? Expliquez brièvement son intérêt.

Q30 : Quel est l'usage du protocole spanning tree ?

Q31 : Citez une solution de supervision de l'infrastructure réseau

ToIP :

Q32 : La structure doit équiper les bureaux des personnels de téléphones IP connectés sur un sous-réseau spécifique. Malheureusement les locaux sont anciens et ils manquent de prises réseaux (RJ45) ainsi que de prises électriques. Que pouvez-vous mettre en place pour solutionner cela sans faire intervenir un prestataire de câblage? Comment devra être paramétré alors le réseau ?

Infrastructure

Q33 : Dans notre structure quel pourrait être l'intérêt de la virtualisation ? Expliquez brièvement pourquoi ?

Q34 : Quel protocole peut-on utiliser pour permettre à tous les utilisateurs (administratifs et élèves) d'être affectés dans le bon vlan (administratif ou enseignant) quel que soit l'ordinateur sur lequel ils ouvrent une session ? Quelles sont les conséquences sur l'infrastructure de l'établissement ?

Annuaire :

Le serveur Windows 2012, situé dans le réseau pédagogique, assure les fonctions suivantes : Active Directory et serveur de fichiers.

Q35 : Quels sont selon vous les avantages d'un tel serveur pour gérer les salles pédagogiques ?

Serveur administratif (Ldap et samba)

La gestion du réseau administratif est assurée par un serveur Linux.

Q36 : Quel(s) service(s) pouvez-vous installer pour obtenir un fonctionnement proche du réseau pédagogique ?

DHCP :

Q37 : Que signifie l'acronyme de DHCP ? Expliquez brièvement son rôle ?

Q38 : Où placeriez-vous le(s) serveur(s) DHCP ? Pourquoi ?

VPN Virtual Private Network ou RVP Réseau Virtuel Privé

Q39 : Dans quel cas utiliser un VPN?

Q40 : Un VPN en transport avec entête AH est-il plus sécurisé qu'un VPN en mode tunnel avec un entête ESP ?

3 - Gestion de projets - étude de besoin : 16 pts

Les réponses doivent être synthétiques et claires. Une attention particulière sera apportée à la qualité de la rédaction, à la présentation et à l'orthographe.

1. Décrivez 5 grandes étapes d'un projet informatique

2. Votre supérieur hiérarchique vous demande de déployer une nouvelle salle de formation pour un nouveau cursus atypique. Elle comportera douze postes. Vous avez un délai de deux mois pour cette réalisation. La salle ne dispose d'aucun équipement et n'est pas disponible en continu. Deux collaborateurs peuvent vous aider pour ce projet et seront disponibles à hauteur d'un tiers de leur temps.

2.1. Quels seront les critères que vous reprenez pour réaliser l'achat du matériel?

Critères d'achat:

2.2. Comment réalisez-vous le planning prévisionnel que vous allez soumettre à votre supérieur hiérarchique?

Réalisation du planning :

2.3 - Comment effectuez-vous le reporting à votre supérieur hiérarchique? Quels indicateurs de suivi de projet mettez-vous en place ?

2.4 - Comment validez-vous que la solution déployée répond bien au besoin initial ?

2.5 Finalement un de vos collaborateurs n'est plus disponible au bout d'un mois. Que faites-vous ?

4 – Organisation du support : 16 pts

Les réponses doivent être courtes, claires et synthétiques.

Il sera tenu compte dans la notation de l'orthographe et de la qualité de la rédaction.

- 1- Un utilisateur vient de recevoir un nouveau poste et demande sa mise en service. Décrire toutes les étapes, depuis le déballage du nouveau poste, jusqu'à la mise au rebut de l'ancien poste. La description doit préciser tous les aspects : matériel, logiciels, réseaux, organisationnels...). Ces opérations font appels à plusieurs services, comment garantir leur coordination ? Dans le cas présent, l'utilisateur doit pouvoir obtenir ce service en ne déposant qu'une unique demande, à un seul interlocuteur.

- 2- Un utilisateur n'arrive plus à ouvrir ses documents bureautiques. Dans les dernières actions, il précise avoir reçu un courrier électronique, avec en pièce jointe un document semblant contenir une candidature spontanée. Il se souvient avoir ouvert ce document. Pour signaler l'incident, l'utilisateur se connecte avec son navigateur qui lui affiche alors un ensemble de publicités. Il se déconnecte et décide de se connecter avec ses identifiants sur le poste d'un de ses collègues, le problème est identique, il contacte alors l'assistance par téléphone.
- En cours de signalement, il constate, au milieu de ses documents, la présence d'un fichier qu'il n'a pas créé. Ce document lui indique qu'un code est nécessaire pour retrouver ses documents bureautiques et qu'il devra payer une rançon pour l'obtenir.
- En tant que membre de l'équipe support utilisateur, quelle serait votre démarche pour dépanner cet usager ?

- 3- Un technicien très sollicité, notamment sur la partie réseau et supervision, doit partir d'ici trois mois, Ayant à cœur le travail bien fait, il souhaite organiser au mieux son départ. Que pourriez-vous lui suggérer pour ne pas vous retrouver dans une situation difficile après son départ ?

5 - Compréhension d'un texte en anglais avec questions en français, réponses attendues en français. 8 points.

À l'aide du texte en ANNEXE 1 :

Question 1 : Qu'est-ce qu'un « Dorkbot » ?

Question 2 : Lorsque vous recevez l'avis en « Annexe1 », quelles actions menez-vous pour protéger les machines clientes ?

ANNEXE 1

Alert (TA15-337A) → <https://www.us-cert.gov/ncas/alerts/TA15-337A>

Dorkbot

Original release date: December 03, 2015

[Print Document](#)

[Tweet](#)

[Like Me](#)

[Share](#)

Systems Affected

Microsoft Windows

Overview

Dorkbot is a botnet used to steal online payment, participate in distributed denial-of-service (DDoS) attacks, and deliver other types of malware to victims' computers. According to Microsoft, the family of malware used in this botnet "has infected more than one million personal computers in over 190 countries over the course of the past year." The United States Department of Homeland Security (DHS), in collaboration with the Federal Bureau of Investigation (FBI) and Microsoft, is releasing this Technical Alert to provide further information about Dorkbot.

Description

Dorkbot-infected systems are used by cyber criminals to steal sensitive information (such as user account credentials), launch denial-of-service (DoS) attacks, disable security protection, and distribute several malware variants to victims' computers. Dorkbot is commonly spread via malicious links sent through social networks instant message programs or through infected USB devices.

In addition, Dorkbot's backdoor functionality allows a remote attacker to exploit infected system. According to Microsoft's analysis, a remote attacker may be able to:

- Download and run a file from a specified URL;
- Collect logon information and passwords through form grabbing, FTP, POP3, or Internet Explorer and Firefox cached login details; or
- Block or redirect certain domains and websites (e.g., security sites).

Impact

A system infected with Dorkbot may be used to send spam, participate in DDoS attacks, or harvest users' credentials for online services, including banking services.

Solution

Users are advised to take the following actions to remediate Dorkbot infections:

- *Use and maintain anti-virus software* – Anti-virus software recognizes and protects your computer against most known viruses. Even though Dorkbot is designed to evade detection, security companies are continuously updating their software to counter these advanced threats. Therefore, it is important to keep your anti-virus software up-to-date. If you suspect you may be a victim of Dorkbot, update your anti-virus software definitions and run a full-system scan. (See [Understanding Anti-Virus Software](#) for more information.)
- *Change your passwords* – Your original passwords may have been compromised during the infection, so you should change them. (See [Choosing and Protecting Passwords](#) for more information.)
- *Keep your operating system and application software up-to-date* – Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. You should enable automatic updates of the operating system if this option is available. (See [Understanding Patches](#) for more information.)
- *Use anti-malware tools* – Using a legitimate program that identifies and removes malware can help eliminate an infection. Users can consider employing a remediation tool (see example below) to help remove Dorkbot from their systems.
- *Disable Autorun* – Dorkbot tries to use the Windows Autorun function to propagate via removable drives (e.g., USB flash drive). You can disable Autorun to stop the threat from spreading.

Microsoft

<http://www.microsoft.com/security/scanner/en-us/default.aspx>(link is external)

The above example does not constitute an exhaustive list. The U.S. Government does not endorse or support any particular product or vendor.

References

- [Microsoft Malware Protection Center – Worm: Win32/Dorkbot](#)(link is external)
- [Microsoft Malware Protection Center – Microsoft assists law enforcement to help disrupt Dorkbot botnets](#)(link is external)

Revisions

- December 3, 2015: Initial Publication
