Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Infrastructure Réseaux

Examen — mai 2018

Durée : 1h30 — Documents autorisés

1 – 9pts En tant qu'auditeur dans une société de sécurité, vous êtes amené à configurer votre machine portable de manière à :

- ▷ vous connecter au réseau de l'entreprise pour réaliser vos détections de vulnérabilités : vous devez être capable de joindre les machines de l'entreprise et d'utiliser l'infrastructure réseau qu'elle fournit ;
- ▷ disposer d'une connexion privée passant par le réseau 4G fourni par votre société d'audit.

Sur votre portable vous disposez :

- □ d'une interface `vers4g` qui exploite une clé 4G et permet de se connecter à l'extérieur de l'entreprise ;
- □ d'une interface `eth0` connectée par ethernet au réseau de l'entreprise ;

Le réseau de l'entreprise est le suivant :

- adresse réseau : `193.50.18.128/25` ;
- adresse passerelle : `193.50.18.254` ;
- serveur DNS : `193.50.18.53` ;
- un serveur DHCP est configuré et offre la plage d'adresse `193.50.18.100-193.50.18.120` à ses clients ;

Le réseau 4G est le suivant :

- adresse réseau : `164.81.1.0/24` ;
- adresse passerelle : `164.81.1.254` ;
- serveur DNS : `164.81.1.4` ;
- un serveur DHCP est configuré et offre la plage d'adresse `164.81.1.100-164.81.1.150` à ses clients ;

On considérera que le réseau de la société d'audit correspond au réseau 4G.

Questions :

a. Sachant que : *(1pt)*

- ◇ votre portable est automatiquement configuré par DHCP lors de la connexion dans le réseau de l'entreprise ;
- ◇ vous installez des programmes spécifiques de l'entreprise à auditer qui peuvent utiliser des adresses de serveurs comme le DNS incluse dans le programme et n'utilisant pas la configuration de la pile TCP/IP ;

Donnez la configuration permettant de rediriger votre trafic DNS vers le serveur de votre choix (par exemple le serveur `8.8.8.8`).

b. Pour des raisons de confidentialité, tout le trafic Web non sécurisé vers le port 80 doit passer par le réseau 4G et celui sécurisé vers le port 443 doit passer par le réseau de l'entreprise. *(2pts)*
Donnez la configuration à appliquer sur votre portable pour le faire.

c. L'auditeur voudrait pouvoir lancer un navigateur tout en étant garanti que tout ce que communique ce navigateur passe par l'interface 4G. *(2pts)*
Donnez la configuration réseau utilisant les « *netns* » capable de rediriger l'intégralité du trafic du navigateur.
On considérera que par défaut les communications du portable de l'auditeur passe par le réseau de l'entreprise. Vous expliquerez votre configuration.

d. À la place de la clé 4G et de son interface, vous disposez d'un tunnel GRE dont l'extrémité est dans votre société sur le poste `164.81.1.123`, et auquel vous accéderez par le réseau de l'entreprise. *(2pts)*
Donnez la configuration de votre portable pour utilisez le tunnel et redirigez le trafic Web port 80 par ce tunnel, et donc, par la société.
Le trafic Web port 443 continuera à passer par le réseau de l'entreprise.

e. Est-ce que le trafic du tunnel est facile à détecter par l'entreprise ? Comment le rendre « confidentiel » ? *(1pt)*

f. Pour tester une vulnérabilité, l'auditeur voudrait envoyer depuis son portable des paquets encapsulés en 802.1Q pour le VLAN 1. *(1pt)*
Donnez la configuration qu'il doit réaliser sur son portable pour le faire.

2 – 2pts Le réseau d'une entreprise est configuré de la manière suivante :
- □ réseau `123.45.67.0/24` ;
- □ plage d'adresses données par le DHCP à ses clients : `123.45.67.2-123.45.67.31` ;

Un serveur applicatif dispose de deux adresses `123.45.67.1` et `123.45.67.50`.

Indiquez comment les clients autoconfigurés par le serveur DHCP utiliseront l'adresse IP du serveur applicatif `123.45.67.31` et les autres machines configurées de manière statique utiliseront l'adresse IP du serveur applicatif `123.45.67.50`.
Est-ce possible et comment doit-être configuré le serveur applicatif pour utiliser l'adresse correcte pour contacter chaque catégorie de machine ?
Vous donnerez également comment doit être choisie l'adresse statique des machines utilisant `123.45.67.50`.
Quelle sera l'adresse par défaut utilisée par le serveur applicatif ?

3 – 2pts Dans le cas d'une attaque au travers de BGP où une AS malveillante annonce un réseau qui ne lui appartient pas afin de détourner le trafic à sa destination, que peut faire l'AS légitime pour rediriger le trafic vers son réseau en utilisant des annonces BGP ?

Vous utiliserez les informations suivantes :
- ▷ le réseau annoncé par l'AS légitime 1935 est `164.81.56.0/26` ;
- ▷ l'AS menant l'attaque est l'AS1234.

4 – 4pts Dans un réseau d'interconnexion on a capturé le trafic suivant :

```
02:12:26.504157 IP (tos 0xc0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 92)
    10.0.0.253.520 > 224.0.0.9.520:
   RIPv2, Response, length: 64, routes: 3
     AFI IPv4,          0.0.0.0/0 , tag 0x0000, metric: 16, next-hop: self
     AFI IPv4,       164.81.10.0/24, tag 0x0000, metric: 16, next-hop: self
     AFI IPv4,   193.50.1.0/24, tag 0x0000, metric: 16, next-hop: self
   0x0000:  45c0 005c 0000 4000 0111 8dcb 0a00 00fd  E..\..@.........
   0x0010:  e000 0009 0208 0208 0048 3e54 0202 0000  .........H>T....
   0x0020:  0002 0000 0000 0000 0000 0000 0000 0000  ................
   0x0030:  0000 0010 0002 0000 ac10 0100 ffff ff00  ................
   0x0040:  0000 0000 0000 0010 0002 0000 c0a8 6400  ..............d.
   0x0050:  ffff ff00 0000 0000 0000 0010            ............
```

a. À quoi sert ce paquet ? *(1pt)*

b. À quoi sert l'adresse « `224.0.0.9` » et à quoi correspond la valeur « `520` » ? *(1pt)*

c. Quelle information importante est transmise dans ce paquet concernant les réseaux dont l'adresse est indiquée dans le corps du paquet ? *(2pt)*

5 – 3pts

a. Pourquoi peut-on présenter MPLS comme un VPN ? Et pourquoi ce n'est pas la même chose ? *(1pt)*

b. Pourquoi la capacité d'un tunnel L2TPv3 à étendre un réseau local n'est pas suffisante et pourquoi peut-il être intéressant de le combiner à MPLS ? *(1pt)*

c. Est-il possible de détecter si, pour une communication, on passe par un tunnel et comment ? *(1pt)*