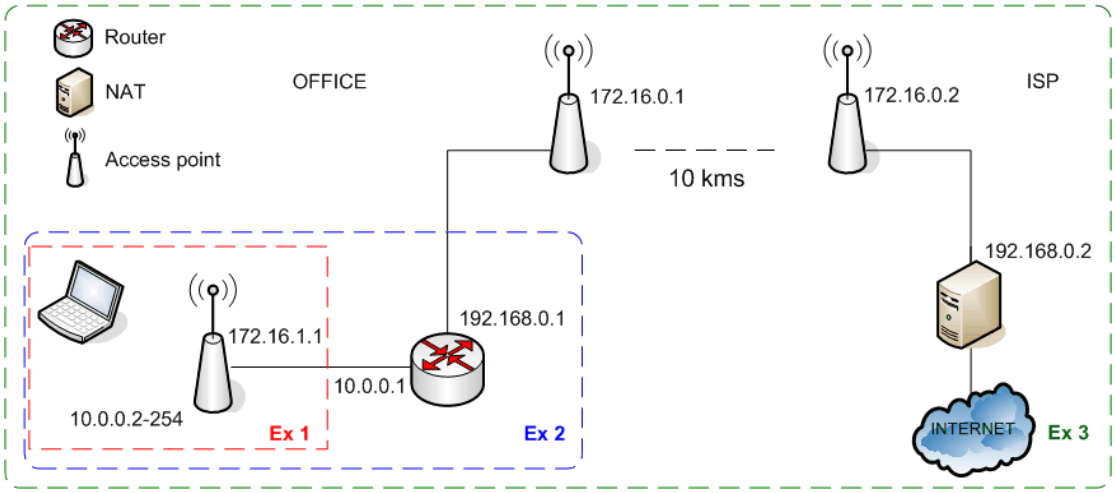
ITRAINONLINE MMTK

Notes sur les exercices : Sécurité sans fil

Préparé par : Alberto Escudero Pascual IT+46



Considérons le scénario suivant : un ordinateur portable est connecté à un réseau local au bureau. Dans l'exemple 1, par un point d'accès; dans l'exemple 2, il reçoit son adresse IP par un serveur DHCP . Tout le bureau est connecté à l'Internet par un lien point à point jusqu'au fournisseur. Le lien sans fil point à point se compose de deux points d'accès qui agissent comme des passerelles.

Le routeur frontière du fournisseur de service et un serveur NAT (exemple 3)

Exercice 1: confidentialité et intégrité des données

Considérez le diagramme (Ex1) ou est connecté le portable dans le réseau sans fil du bureau.

Question 1: Comment pouvez-vous garantir la confidentialité et l'intégrité des données?

- *Quelles fonctions pouvez-vous mettre en œuvre et comment?*

  Sujets possibles de discussion:

  Mettez en œuvre WPA2-Enterprise pour assurer tout le cryptage du niveau lien IEEE 802.1X

  Mettez en œuvre WPA2-Personal et convenez d'un secret partagé au bureau. Discutez si cela est approprié.

  Entraînez votre équipe à comprendre quels services est à risque et utilisez les logiciels de sécurité SANS cryptage.

  Mettez en œuvre une solution VPN et forcez les clients à communiquer via le concentrateur VPN.

- *Discutez de toutes les alternatives possibles pour assurer la confidentialité des données dans le premier saut (entre le portable et le point d'accès)*

  Sujets possibles de discussion:

Les pours et les contres de l'utilisation de WPA2 avec et sans IEEE 802..1X, désactivez le cryptage, introduisez une solution VPN (compatibilité, coûts), gestion du réseau, etc.

Maintenant, regardez l'autre diagramme (Ex3)

Question 3: Comment le fournisseur de service peut-il garantir la confidentialité et l'intégrité des données dans le lien point à point?

- Discutez des avantages et désavantages de chacune des solutions.

Sujets possibles de discussion:

Le fournisseur devrait mettre en œuvre un système d'identification dans les liens Point à point pour éviter l'intrusion illicite sur le réseau.

Le fournisseur peut décider de NE PAS utiliser le cryptage à cause de :

a) Lois en vigueur (est-ce légal?)

b) les difficultés physiques pour un utilisateur non autorisé d'écouter le trafic (les antennes sont très hautes, bien dirigées, etc.)

c) réduire le travail de gestion de réseau

Exercice 2: Identification – contrôle de l'accès

Considérant le diagramme (Ex2): Le routeur fournit les adresses IP aux clients sans fil par le DHCP.

Question 1: Comment pouvez-vous empêcher des usagers non autorisés d'obtenir une adresse IP du réseau?

Sujets possibles de discussion:

Mettre en œuvre l'identification au point d'accès au moyen de WPA ouWPA2

Utilisez des adresses IP statiques et surveillez les requêtes DHCP (rendre les choses un peu plus difficiles pour les attaques)

Ne pas diffuser le SSID et limitez la couverture sans fil (rendre les choses un peu plus difficiles pour les attaques)

Question 2: Comment pouvez-vous empêcher des usagers non autorisés de rejoindre l'Internet par votre réseau?

Sujets possibles de discussion:

Bloquer le trafic IP dans le routeur du bureau

Permettre seulement certaines adresses MAC/IP dans le routeur

Mettre en œuvre une solution de type portail captif dans le routeur du bureau

Considérant le diagramme (Ex3): le fournisseur de services fourni la connectivité au moyen d'un serveur NAT.

Question 3: Comment le fournisseur peut-il assurer que seulement votre bureau est connecté à son réseau?

Sujets possibles de discussion:

Permettre seulement le trafic IP entrant provenant de l'adresse MAC du routeur du bureau

Mettre en œuvre un portail captif dans le serveur NAT en permettant l'identification par usager

Assurer que le point à point force l'identification partout

Exercice 3: Disponibilité et prévention du refus de service

Considérant les diagrammes de bureau (Ex1, Ex2) et celui du fournisseur (Ex3)

Question 1 : Décrivez ce qui peut tourner mal dans chaque saut de communication. Qu'est-ce qui peut rendre le réseau non disponible?

Sujets possibles de discussion:

« *Radio Jamming* » dans les deux liens sans fil

Usagers non autorisé associé avec n'importe quel point d'accès pour envoyer du trafic

Des logiciels malicieux inondent les liens sans fil

Usagers non autorisés imitent les routeurs (détournement IP/MAC)

Usagers non autorisés imitent le point d'accès (détournement du canal radio)

Question 2 : Décrivez comment résoudre chacun des problèmes de sécurité et qui devrait être responsable de mettre en œuvre les solutions?

Sujets possibles de discussion:

« *Radio Jamming* » dans les deux liens sans fil : surveillez périodiquement vos liens sans fil, reportez les attaques à l'autorité des télécommunications

Usagers non autorisés s'associent à n'importe quel point d'accès et envoi du trafic malicieux : mettez en œuvre WPA2, introduisez des politiques d'organisation du trafic dans les routeurs et les points d'accès, limitez la couverture de votre réseau sans fil

Des logiciels malicieux inondent les liens sans fil: surveillez le trafic IP, introduisez des systèmes de détection des intrusions, introduisez l'organisation du trafic, déconnectez les stations infectées.

Des usagers non autorisés imitent les routeurs (détournement IP-MAC): mettez en place l'identification dans vos liens point à point, surveillez le SNR pour détecter les gros changements

Des usagers non autorisés imitent un point d'accès (d.tournement du canal radio): mettez en oeuvre l'identification dans vos liens Point à point, surveillez le SNR pour détecter les gros changements

Question 3 : Pensez à un scénario concret (hôpital, école, télécentre, etc..) et décrivez les besoins en termes de mesures de sécurité à prendre.