



Gardien Virtuel

s é c u r i t é
i n f o r m a t i q u e

Vérification WIFI-Laval

Ce document est offert par:

Patrick Boucher, CISA, CISSP
Analyste en sécurité informatique

Gardien Virtuel Inc.
Direct: 514-246-4836
Sans-frais 1-888-377-7890 x 701
Courriel: info@gardienvirtuel.com

Droit d'auteur 2006 par Gardien Virtuel Inc., Ce document est ouvert au public. La distribution de version modifiée de ce document est interdite sans l'autorisation écrite de Gardien Virtuel Inc.

La dernière version de ce document se trouve à l'URL suivant:

<http://www.gardienvirtuel.com>

Détails du document

Type:	Rapport de test de sécurité
Version:	1.0: Finale
Date de création:	Mercredi 31 mai 2006
Dernière modification:	lundi 14 août 2006

Table des matières

Sommaire exécutif.....	3
Méthodologie.....	4
Recherche réseau WIFI.....	4
Équipement utilisé.....	4
Informations générales.....	5
Définitions.....	5
Cible: Laval, Québec.....	6
Quelques statistiques de la ville de Laval.....	6
Délimitation des secteurs.....	7
Délimitation des secteurs (suite).....	8
Restriction de détection.....	8
Portée du projet.....	9
Échéancier du projet.....	9
Résultats de l'analyse	10
Résultats détaillés de l'analyse.....	10
Configuration recommandée.....	12
Références.....	13

Sommaire exécutif

L'objectif de cet exercice est de sensibiliser la population ainsi que les entreprises à la sécurité informatique et aux bonnes pratiques.

Depuis quelque temps, il est de plus en plus populaire de se connecter à l'Internet grâce à la technologie des routeurs sans-fils. Très pratiques, les réseaux sans-fils utilisent les ondes radio-électriques, au lieu des câbles, pour la transmission de données.

Ces routeurs sans-fils demandent une configuration et certaines connaissances informatiques afin de les sécuriser correctement.

Gardien Virtuel Inc. voulait prendre le pouls du degré de sécurité de la technologie sans-fils à Laval. Les résultats obtenus sont très révélateurs. De façon générale 43% des réseaux sans-fils découverts ne sont pas sécurisés, donc complètement ouverts et disponibles pour tous. Toutes les informations transmises entre le poste client et le réseau Internet ne sont protégées d'aucune façon. Il est donc possible pour une personne, avec de mauvaises intentions, de compromettre l'intégrité et la confidentialité de presque toutes les données transmises depuis le poste client.

Plusieurs solutions existent pour protéger ces informations. Vous en trouverez quelques une dans les prochaines pages.

Vous trouverez dans les prochaines pages de ce document tous ce qui concerne l'opération "Wardriving Laval"!

Méthodologie

Recherche réseau WIFI

Afin de collecter le maximum de point d'accès sans fils sur l'île de Laval, les analystes de **Gardien Virtuel Inc.** ont circulé dans les rues de Laval avec un ordinateur portable, une carte réseau sans-fil et une antenne activée.

La collecte de donnée s'est effectuée principalement dans les grandes artères de la ville puis dans certains cartiers précis afin d'augmenter le nombre de point d'accès sans-fils détectés. L'objectif consistait à avoir un nombre suffisant de points d'accès pour chaque zone visée.

En plus des zones géographiques de Laval, nous avons porté une attention particulière au fait d'obtenir des statistiques sur les zones résidentielles, commerciales et industrielles.

Le logiciel Netstumbler, application pour la plate forme Windows, a été utilisé pour ce projet. Pour effectuer le balayage des ondes, l'application envoie une demande de connexion plusieurs fois par seconde à tous les points d'accès sans-fils. Ceux-ci répondent donc à ces requêtes avec l'information nécessaire pour établir une connexion. Cette action permet au logiciel de comptabiliser l'information des points d'accès sans-fils.

Équipement utilisé

- Antenne à gain 9 DBI
- Carte WIFI pour ordinateur portable
- Carte routière de Laval
- Logiciel « Netstumbler »
- Ordinateur portable
- Système de positionnement par satellite GPS (Garmin PC18)
- Voiture

Informations générales

Définitions

802.11 : Ce numéro réfère à la norme IEEE 802.11 (ISO/CEI 8802-11) laquelle est un standard international décrivant les caractéristiques d'un réseau local sans fil.

AP : Access Point ou Point d'accès en français. Équipement réseau permettant de lier un réseau câblé vers un réseau sans-fils. Sert de pont entre les ordinateurs munis de carte d'accès sans-fils et un réseau local ou Internet.

PCMCIA : (pour Personal Computer Memory Card International Association), ou PC Card, est un format de carte d'extension ultra-plat, destiné aux ordinateurs portables.

Netstumbler: Logiciel utilisé pour écouter les ondes radio des points d'accès sans-fils et en détecter la présence.

Wardriving : Le terme "WarDriving" désigne l'action de recherche de point d'accès sans-fils avec l'utilisation d'une voiture (d'où le terme Driving). Pour l'instant aucun terme français n'existe.

WEP : Wired Equivalent Privacy (abrégié WEP) est un protocole désuet pour sécuriser les réseaux sans-fil de type Wi-Fi. Par conséquent les réseaux sans-fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans-fils une confidentialité comparable à celle d'un réseau local filaire classique. Cependant, plusieurs faiblesses graves ont été identifiées par les cryptologues. Le WEP a donc été supplanté par le WPA en 2003, puis par le WPA2 en 2004 (WPA2 est la version de la norme IEEE 802.11i certifiée par la Wi-Fi Alliance). Malgré ses faiblesses intrinsèques, le WEP fournit un niveau de sécurité *minimal qui peut décourager les attaquants les moins expérimentés*. Il est à noter que le niveau de protection offert est loin du niveau recommandé par Gardien Virtuel.

WPA : Wi-Fi Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type Wi-Fi. Ils ont été créés en réponse aux nombreuses et sévères faiblesses que des chercheurs ont *trouvées dans le mécanisme WEP*.

WIFI : Technologie de réseau informatique sans-fils servant de moyen d'accès à Internet.

Cible: Laval, Québec

Notre objectif est de sensibiliser la population générale et les entreprises à la sécurité informatique. Pour ce faire, nous avons réalisé un grand balayage des réseaux sans-fils de la ville de Laval.

Quelques statistiques de la ville de Laval

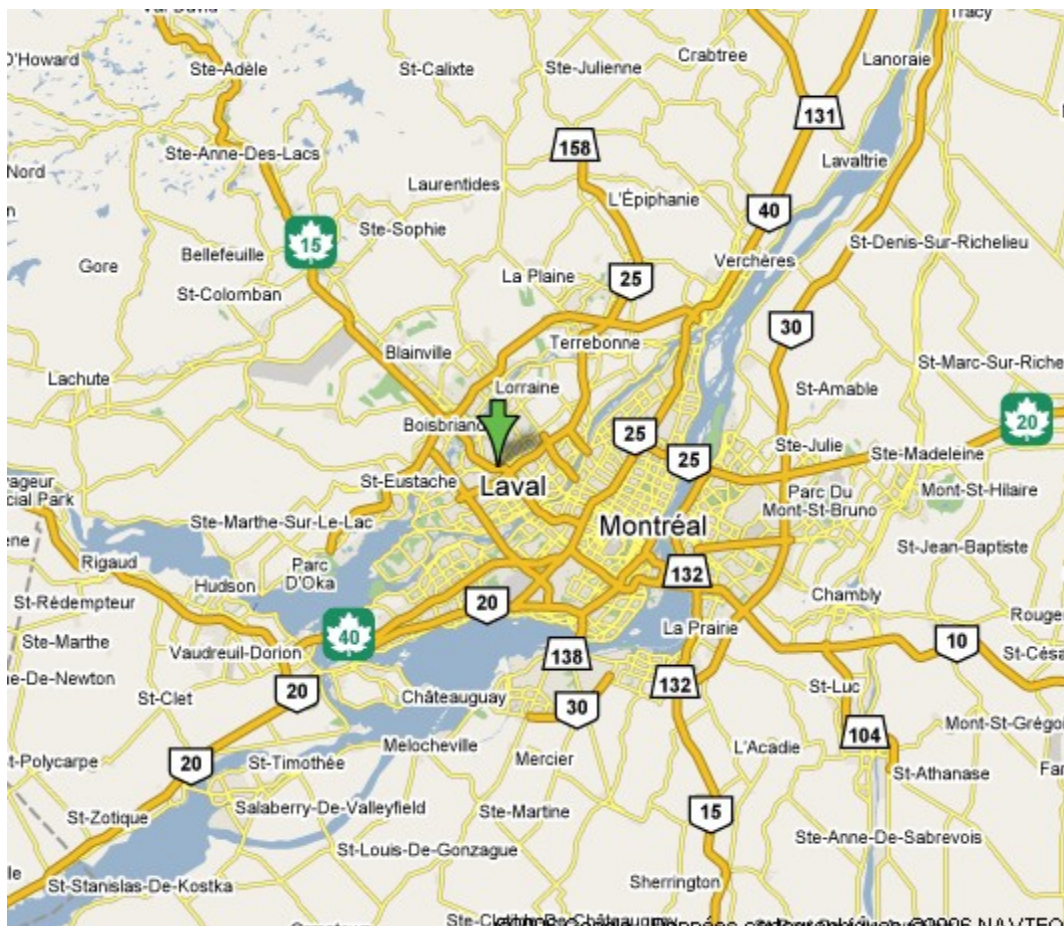
Superficie Totale: **247.07 km²**

Population (2006): **365 623**

Revenu disponible par habitant en 2004 :

Laval: **30 623 \$**

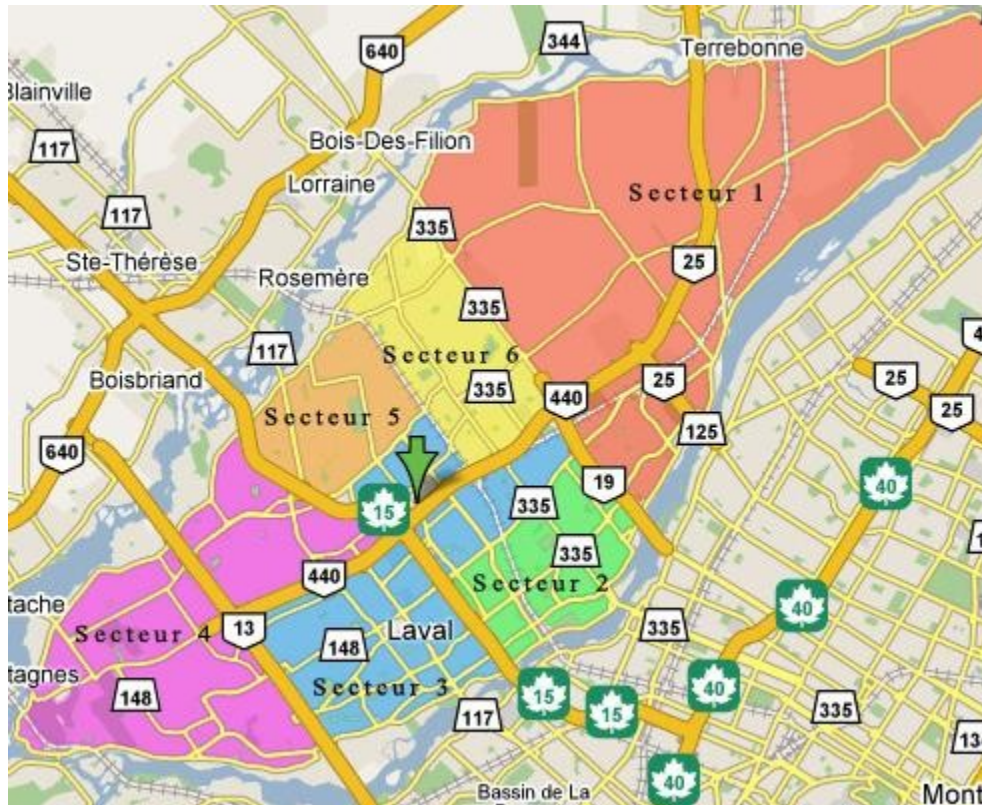
Québec: **28 595\$**



Délimitation des secteurs

<i>Secteur</i>	<i>Nom</i>	<i>Description</i>
1	Saint-François Saint-Vincent-de-Paul Duvernay	Secteur délimité à l'est de la route 19.
2	Laval des rapide Pont-Viau	Secteur délimité au nord par le boul. Saint-Martin, à l'est par la route 19, au sud par la rivière des prairies et à l'ouest par l'autoroute 15
3	Chomedey	Secteur délimité au nord par le boul. Dagenais, à l'est par la rail de chemin de fer, au sud par le boul. Saint-Martin et à l'ouest par l'autoroute 15. Secteur délimité au nord par l'autoroute 440, à l'est par l'autoroute 15, au sud la rivière des prairies et l'ouest par l'autoroute 13
4	Fabreville Laval-Ouest Laval-sur-le-Lac Sainte-Dorothée	Secteur délimité à l'est de l'autoroute 13. Secteur délimité au nord par la rivière des mille îles, à l'est par l'autoroute 13, au sud par l'autoroute 440 et à l'ouest par l'autoroute 15
5	Sainte-Rose	Secteur délimité au nord par la rivière des mille îles, à l'est par la rail de chemin de fer, au sud par l'autoroute 440 et à l'ouest par l'autoroute 13.
6	Auteil Vimont	Secteur délimité au nord par la rivière des mille îles, à l'est par l'autoroute 19, au sud par l'autoroute 440 et à l'ouest par la rail de chemin de fer.

Délimitation des secteurs (suite)



Restriction de détection

Compte tenu des éléments suivants, il est impossible de déterminer avec exactitude le nombre de point d'accès :

- Point d'accès débranché ou inopérant au moment du balayage
- Point d'accès hors d'accès de la rue
- Réseau sans-fils utilisant une norme ou technologie non balayée.

Cependant les chiffres obtenus représentent un portrait fidèle de la réalité.

Portée du projet

Il est important de mentionner que dans le cadre de ce projet, aucune information concernant les réseaux en question n'a été capturée, même lorsqu'il était possible de pirater des données privées des réseaux insécurisés.

Les seules informations obtenues sur les réseaux sont les suivantes :

- Nom d'identification du réseau (SSID)
- Utilisation de l'encryption (WEP, WPA) active ou non
- Localisation du réseau par GPS

À titre d'experts en sécurité informatique, les auteurs de ce rapport ne voulaient pas pirater des données privées, mais seulement sensibiliser la population générale et les entreprises aux nombreuses failles existantes dans les réseaux WIFI. Les statistiques et situation de sécurité sont probablement les mêmes à Montréal, à Québec, à Sherbrooke, etc...

Échéancier du projet

Date de début : **Jeudi le 01 juin 2006**

Date de fin: **Vendredi le 14 juillet 2006**

Résultats de l'analyse

Les résultats obtenus sont très révélateurs.

Nous avons répertoriés 5880 point d'accès sans-fils sur l'île de Laval, 43% de ceux-ci n'utilisent aucun protocole de sécurisation et sont complètement ouverts.

Par secteur, le pourcentage des réseaux sans-fils répertoriés « ouvert » varient entre 39% et 48%.

Nous pouvons constater que le pourcentage de réseaux sans-fils non-sécurisé dans les secteurs commerciaux sont les plus élevés. 60% des réseaux sans-fils dans les secteurs commerciaux ne sont pas sécurisés, comparativement à 43% dans les secteurs résidentiels et 28% dans le secteur industriel.

Résultats détaillés de l'analyse

En nombre

<i>Secteur</i>	<i>Point d'accès sans-fils</i>	<i>Avec chiffrement Protégés</i>	<i>Ouvert Sans protection</i>
1	830	430	400
2	659	390	269
3	1983	1201	782
4	1163	655	508
5	562	301	261
6	683	371	312
Total	<u>5880</u>	<u>3348</u>	<u>2532</u>
Industriel	246	176	70
Commercial	286	115	171
Résidentiel	5348	3057	2291

Résultat en pourcentage:

<i>Secteur</i>	<i>Point d'accès</i>	<i>Avec chiffrement %</i>	<i>Ouvert %</i>
1	830	52%	48%
2	659	59%	41%
3	1983	61%	39%
4	1163	56%	44%
5	562	54%	46%
6	683	54%	46%
Total	<u>5880</u>	<u>57%</u>	<u>43%</u>
<i>Industriel</i>	246	72%	28%
<i>Commercial</i>	286	40%	60%
<i>Résidentiel</i>	5348	57%	43%

Configuration recommandée

Voici les quelques suggestions afin de sécuriser un point d'accès Sans-fil :

- Modifier le SSID (Service Set Identifier) pour un nom unique exemple: (LK-190)
La modification du SSID vous permet de vous distinguer des autres réseaux de vos voisins.
- Désactiver la fonction « SSID Broadcast »
Vous connaissez votre identification, il est donc inutile de l'annoncer à tous.
- Activer le filtrage par MAC.
Cette fonction permet de bloquer l'accès à votre routeur par d'autres ordinateurs que le vôtre. (Voir le lexique pour MAC)
- Activer le chiffrement WPA-PSK ou WPA-Personel (Équivalent plus avancé de WEP)
Ceci est la fonction qui permet véritablement de chiffrer et protéger vos communications entre votre ordinateur et le routeur sans fils.

Liens Internet pertinents pour sécuriser un réseau sans-fils :

http://www.microsoft.com/windowsxp/using/networking/learnmore/bowman_05february10.msp

Guide de gestion et des contrôles d'accès:

https://www.isiq.ca/fr/Guides/PME/128_acces.html

Références

Statistique Canada

Institut de la statistique du Québec

Ministère des affaires municipales

Les affaires – 20 mai 2006

maps.google.com