UQAC
Université du Québec
à Chicoutimi

8INF135 - Sécurité informatique
Travail Pratique 2 : Crypto et sécurité des réseaux

Rapport de sécurité

Remettre à : Valère Plantevin
Le : Dimanche 12 Décembre 2017

Par

Haerinck Guillaume
Aziz Tekaya
Nicolas Noret

Checklist de la sécurité

Besoins

L'armée a besoin d'un serveur le plus sécurisé possible pouvant permettre de communiquer des secrets militaires sans qu'ils soient compromis, cela implique:

- Certitude que le paquet est bien arrivé
- Certitude que personne n'a pu lire le paquet
- Certitude que personne n'a pu modifier le paquet
- Certitude de qui a envoyé le paquet

Leur statut les libère des contraintes liés à l'interdiction d'utiliser des algorithmes cryptographiques tels que RSA-4096.

Assets

Matériel

Le matériel est adéquat avec la demande, nombreux et de qualité il comprend:

2 pare-feu matériels
Ils sont basés sur le logiciel iptables

4 serveurs
- 1 réservé à la communication avec Ottawa
- 1 pour vous et les membres du personnel ayant accès aux secrets militaires
- 1 pour vos mécaniciens
- 1 pour les données des scientifiques

Plusieurs switches gérant les VLANs

Plusieurs routeurs

51 ordinateurs
- 1 pour l'administrateur réseau
- 15 pour le personnel
- 15 pour les scientifiques
- 20 pour le reste de la base

Logiciels

Les serveurs sont configurés sous linux.
Les ordinateurs sont sous windows.

Données

Ils s'agit de secrets militaires, transmis sous forme de textes.

Moyens de communications

L'architecture est pour le moment inexistante, mais des besoins spécifiques ont été formulés:

Sur les 15 membres de personnels

- 5 avec des accès complets à tout le réseau y compris aux informations sécurisées.
- 10 mécaniciens sans accès aux secrets militaires, mais avec accès aux différents schémas techniques de la base.

Sur les 15 scientifiques civils

- Aucun accès aux secrets militaires
- Ils possèdent leurs propres données sécurisées
- Il ont un accès exclusif au serveur de calcul

Risques

L'installation se trouve dans une zone de guerre, et protège des informations convoités par des états, ce qui implique les risques suivants:

Risque	**Attaque**
Prise de contrôle du serveur	Accès physique à l'interface de commande
Employé malicieux	Récupération de données non-autorisés
Perte de disponibilité du serveur	DDos
Destruction des installations	Bombardement

Contre-mesures

Face à chacuns de ces risques, on peut formuler les mesures suivantes:

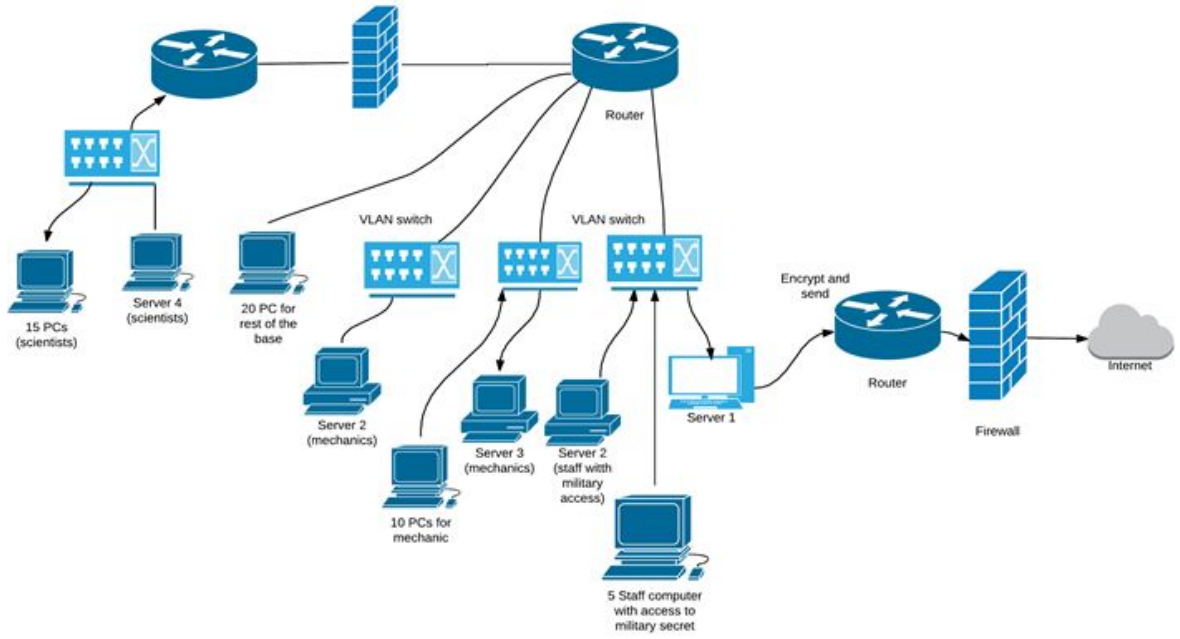
Risque	**Contre-mesure**
Prise de contrôle du serveur	Boucler le serveur dans une DMZ
Employé malicieux	Droit d'accès pour les utilisateurs
Perte de disponibilité du serveur	Utiliser un bon pare-feu
Destruction des installations	Mettre la DMZ en sous-sols

Équilibrages

L’armé possède de fort moyens financiers ce qui ne pose pas de problèmes niveau matériel.

Solution proposée

Architecture



Fonctionnement des applications

On part du principe que les clés publiques RSA ont déjà été partagées, et par extension chacun à accès à sa propre clé privé.

SouthPoleClient

C'est un invite de commande qui récupère les messages entrés par l'utilisateur et les envois, en clair, à l'IP indiqué en utilisant le port indiqué (supposément toujours 29, le port de TCP).

SouthPoleServer

Il écoute avec l'interface indiqué sur le port indiqué (supporte le **multi-threading** tant que le dernier client à se connecter envoi en premier le message). Les messages récupérés sont hashés avec SHA-512 (pour vérifier l'**intégrité** = certitude que personne n'a pu modifier le paquet), puis cryptés avec RSA-4096 avec la clé publique du destinataire (pour assurer la **confidentialité** = certitude que personne n'a pu ouvrir le paquet).

Le message est envoyé sans son hash, par l'interface indiquée en utilisant le port 8080.

Puis le hash est crypté avec RSA-4096 avec sa clé privé (pour vérifier l'**authenticité** = certitude de qui a envoyé le hash), et envoyé à son tour.

OttawaServer

Il écoute sur le port 8080, et décrypte les messages reçus. Puis il hashes avec SHA-512 et compare le hash obtenu de celui envoyé.

Il envoi ensuite les messages à l'adresse IP multicast 239.255.1.1 en utilisant le port 6666