Denis Morency

De: no-reply@www.usherbrooke.ca
Envoyé: 17 avril 2015 09:32
À: Sciences-CentreImpression@USherbrooke.ca
Objet: COMMANDE EXAMENS
Pièces jointes: IFT606_Final_H2015.pdf

TYPE-EXAMEN	FINAL
SIGLE-COURS	IFT606
TITRE-COURS	Sécurité et cryptographie
PROFESSEUR	Mohammed Ouenzar et Marc Verreault
DATE-HEURE	Jeudi 23 avril à 9 h
AUTORISE-PAR	Gabriel Girard, Mohammed Ouenzar et Marc Verreault
NOMBRE-PAGES	14, impression en couleur
NOMBRE-COPIE-PROF	45+2 copies à l'AGES (47)
IMPRESSION-QUESTIONNAIRE	Recto-verso broché
NOMBRE-FEUILLES-BLANCHES	3
NOMBRE-PAPIER-GRAPHIQUE	
NOMBRE-CAHIERS	
CONSENTEMENT-AGES	1
REMARQUES	Impression en couleur. 45 étudiants. 2 copies à l'AGES. Mohammed.Ouenzar@usherbrooke.ca Marc.Verreault@usherbrooke.ca
E-MAIL	
FIRST-NAME	
LAST-NAME	
NICK-NAME	
SPAMSHIELD	true

UNIVERSITÉ DE SHERBROOKE

Université de Sherbrooke

Département d'informatique

IFT 606

Cryptographie et sécurité

Chargés de cours :

Mohammed Ouenzar

Marc Verreault

Examen final

Jeudi 23 avril 2015, 09h00 à 12h00

Attaque, défense, architecture et enquêtes

Consignes :

- Cet examen comprend quatre questions réparties sur 14 pages.
- Assurez-vous que toutes les questions s'y retrouvent.
- Aucune documentation n'est permise.
- L'évaluation compte pour 35% de la note finale.

Nom : _____ Prénom : _____

Signature : _____ Matricule : _____

Question 1 : Politiques au Pare-Feu (défense) 25pts

Le Pare-feu permet de :

1) filtrer les paquets réseaux en les laissant passer ou en les bloquant;
2) d'inspecter les paquets réseaux afin de déterminer des anomalies;
3) de prévenir les menaces à partir de cette inspection (UTM);
4) d'intercepter le trafic dirigé vers l'extérieur («proxy»);
5) de contrôler l'accès aux réseaux via l'identité des machines et utilisateurs.

Dans la fonction UTM, au numéro 3 ci-dessus, on retrouve entre autres les trois méthodes de protection suivantes :

Méthode #1) Méthode SYN Flood Protection

Le principe d'attaque «SYN Flood» est de ne pas compléter les échanges de «handshaking» nécessaires à l'établissement d'une session légitime TCP. L'objectif de l'attaque SYN Flood, est de désactiver un des côtés d'une connexion TCP, ce qui résulte en un ou plusieurs scénarios :

⇒ Le serveur n'accepte plus de nouvelle connexion;

⇒ Le serveur cesse de fonctionner ou ne répond plus;

⇒ L'autorisation entre serveurs est dégradée.

Un bon Pare-Feu devrait protéger contre les attaques «SYN Floods».

Les deux principales technologies pour contrer ce type d'attaques sont : «SYN Cookies» et «TCP Intercept».

SYN Cookies

Réside entièrement sur le serveur. Au lieu de conserver les «SYN requests» dans une file (queue), le serveur utilise une fonction cryptographique pour déterminer le numéro de séquence initial (ISN). Il n'a pas besoin de conserver les paquets SYN et il est en mesure de vérifier les paquets ACK du client en utilisant cette fonction cryptographique.

TCP Intercept

Consiste en une défense basée réseau. Un équipement réseau intercepte la communication au moment où elle s'établit. Le client, qui tente de négocier une connexion TCP avec un serveur, communique en réalité avec cet équipement réseau. Si la négociation se complète et qu'une session TCP est alors ouverte,

l'équipement amorce la négociation du côté du serveur. C'est l'équipement qui est alors affecté par le SYN Flood plutôt que le serveur.

1.1 Quels sont les avantages et inconvénients de la technologie *SYN Cookies* versus *TCP Intercept* (*10 pts*)?

Méthode #2) IP address spoofing protection

Le principe d'attaque «IP spoofing» est d'amener le Pare-Feu à accepter du trafic d'un segment normalement interdit en modifiant l'adresse source de l'entête IP du paquet. Par cette modification, l'attaquant fait croire au Pare-Feu que le paquet provient d'un ordinateur auquel le Pare-Feu fait confiance.

Un bon Pare-Feu devrait protéger contre les attaques «IP spoofing».

La cryptographie (IPsec) est le principal moyen de prévention de ce type d'attaque. Un autre moyen : l'utilisation de listes de contrôle d'accès pour refuser des adresses IP privées sur l'interface interne du Pare-Feu, c'est-à-dire ne pas accepter un paquet provenant de l'externe avec une adresse source du réseau interne.

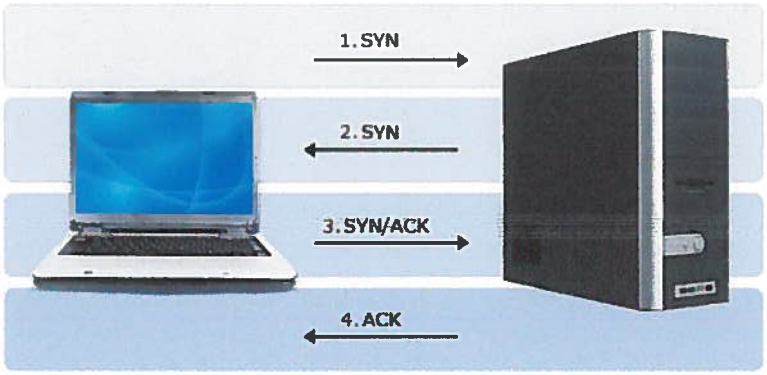
1.2 Expliquez en quoi la protection «IP address spoofing» pourrait aider à protéger des attaques «SYN flooding». (*7 pts*)

Méthode #3) TCP Split Handshake Spoof protection

Cette attaque confond le Pare-Feu afin de faire passer du trafic d'un segment à un autre. Cette attaque combine la négociation TCP (3 way handshake) et l'ouverture de plusieurs connexions simultanément. Le résultat est une attaque de type «TCP spoof» qui permet à l'attaquant de traverser le Pare-Feu pour provoquer l'initiation d'une session par l'ordinateur victime sur celui de l'attaquant. Ce type de «handshaking» est supporté par Microsoft, Apple et Linux.

Qu'est-ce qu'un TCP Split Handshake Spoof?

Un TCP Split Handshake cause un comportement inconsistant en renversant la direction des flux de la négociation comme suit :



1. Le client envoie un paquet SYN au serveur, comme cela se réalise normalement
2. Le client (malicieux) renvoie un paquet SYN au lieu d'un SYN-ACK
3. Le client répond de manière incorrecte avec un SYN/ACK au serveur
4. Le serveur complète la transaction en envoyant un paquet ACK en réponse au SYN/ACK du client

Figure 1: Les étapes de négociation dans une attaque «TCP Split Handshake Spoof»

Un bon Pare-Feu devrait protéger contre les attaques «TCP Split Handshake Spoof».

1.3 À quelle étape de la négociation de la figure précédente les équipements réseaux devraient bloquer l'attaque TCP Split handshake spoof (1, 2, 3 ou 4)? Expliquez votre choix en moins de 20 mots. (*8 pts*)

Question 2 : Questions rafales (défense) 25pts

Quelle est le moyen de défense le plus efficace contre (pour prévenir) les attaques ci-dessous (choisissez la meilleure des deux)?

2.1 Probe/scan via nmap (*2pts*)

[_] One-time password

[_] Bloquer ICMP au Pare-Feu

2.2 Sniffing (*2pts*)

[_] Configurer la sécurité des ports au Pare-Feu et crypter la connexion

[_] Sensibiliser les utilisateurs à ne pas donner d'information

2.3 Buffer overflow attacks (*2pts*)

[_] Durcissement de système d'exploitation et applicatif (incluant la vérification des champs)

[_] Augmenter la complexité requise des mots de passes

2.4 Rogues devices (équipements réseaux connectés par les attaquants (*2pts*)

[_] RADIUS/TACACS+ (authentification d'équipements)

[_] Biométrie

2.5 Man-in-the-middle attack (MITM) (*2pts*)

[_] Rogue device detection

[_] Entre trois personnes, choisir celle qui n'est pas au milieu par écrit

2.6 Cross-site scripting (XSS) (*2pts*)

[_] <script>...NEVER PUT UNTRUSTED DATA HERE...</script>

[_] <script>... password_variable ...</script>

2.7 Hameçonnage courriel (*2pts*)

[_] Séparation des serveurs de fichiers et de courriel

[_] Filtrage applicatif au Pare-Feu

2.8 Rootkit (*2pts*)

[_] chmod ug+s /bin/bash; ln /bin/bash /usr/apache/www/rbc/bin;
echo "backdoor installée" > /usr/apache/www/rbc/bkdoor.log

[_] Mises à jour et durcissement système exploitation et applicatif

2.9 SYN Flood (*2pts*)

[_] «HTTP cookies» et «MOODLE2 intercept»

[_] «SYN Cookies» et «TCP Intercept»

2.10 IP spoofing (*2pts*)

[_] Refuser les paquets reçus à l'interface externe du Pare-Feu qui contiennent une adresse source privée

[_] La cryptographie (IPsec)

2.11 «Social engineering» (*2pts*)

[_] Sensibiliser les utilisateurs

[_] Éliminer les ingénieurs

2.12 «Dumpster diving» (Fouille dans les rebus pour de l'information) (*2pts*)

[_] Cadenasser les déchets

[_] Contrôler l'ensemble du processus de gestion des déchets

2.13 Attaque impliquant toutes les attaques précédentes (*1pt*)

[_] Sensibilisation des utilisateurs

[_] Mettre en place un cadre de gestion de la sécurité

Question 3 : Architecture — 25pts

La figure suivante présente une architecture de sécurité à haut niveau d'une grande banque qui offre à ses employés la possibilité de télétravail.

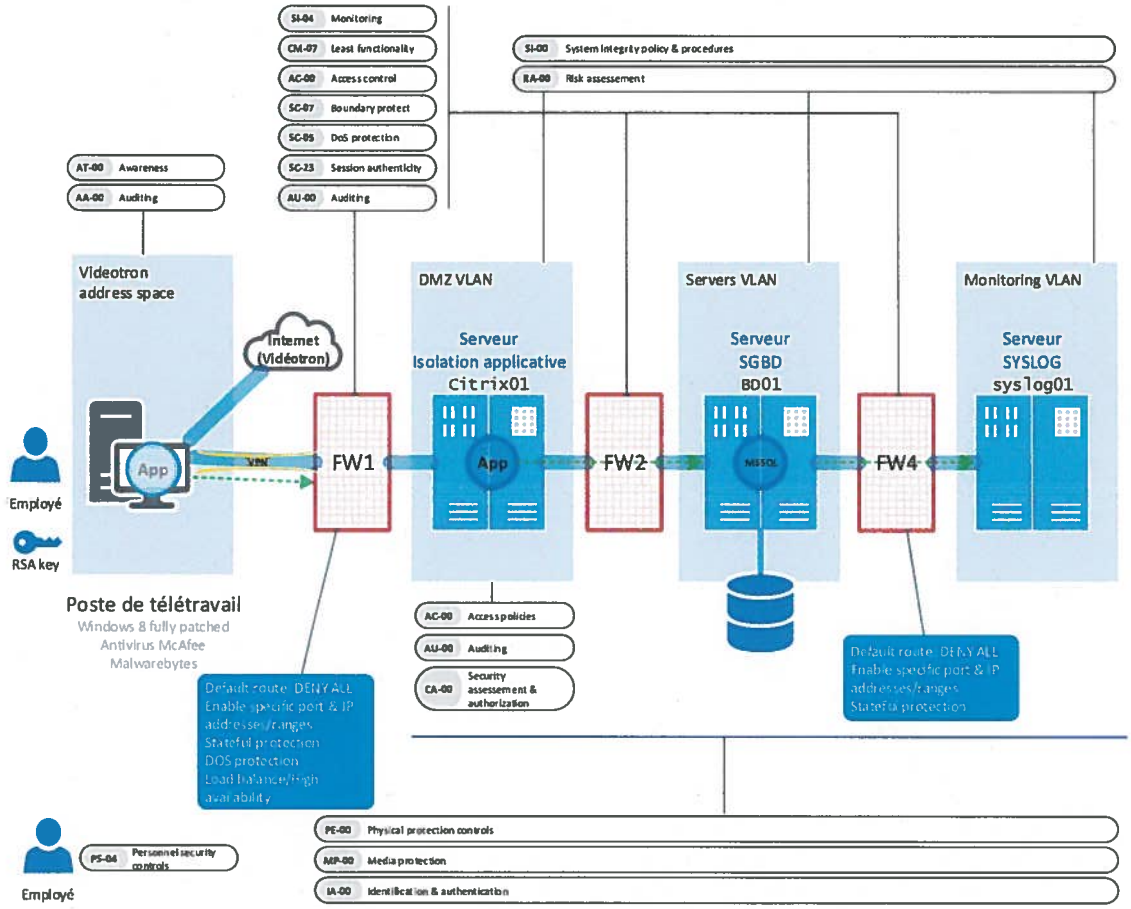


Figure 2: Architecture de sécurité d'une grande banque. La flèche entre le poste de télétravail et le Pare-Feu (FW1) représente la transaction réseau requise (incluant l'authentification) pour mettre en place le VPN.

3.1 Quel est l'équipement/ordinateur le plus susceptible de se faire infecter selon ce scénario? Pourquoi? (*10pts*)

Indice : Chercher là où les menaces sont les plus grandes.

3.2 En fonction de votre évaluation de cette architecture, proposez des améliorations possibles et justifiez-les. (*15pts*)

Question 4 : Enquête — 25pts

L'architecture à haut niveau d'une centrale nucléaire montre les composantes réseaux, les ordinateurs et les composantes de contrôle du refroidissement des barres d'uranium au cœur du réacteur. Il y a deux thermomètres qui envoient un signal à deux ordinateurs qui contrôlent les pompes à eau lourde. Ces pompes permettent de conserver la température du cœur de la centrale à un niveau acceptable.

Lors d'un récent incident, une de ces pompe a été coupée à cause d'une infection du PC du VLAN REACTOR_CTRL_1. On l'a échappé belle mais on souhaite déterminer la cause et on doit légalement documenter cet incident.

Les constats :

Constat #1: XP infecté par un virus sans signature dans l'antivirus sur le VLAN de contrôle #1. L'autre pas infecté. Le PC infecté a temporairement été déconnecté du réseau, mais il presse de le remettre en fonction.

Constat #2: Pas d'antivirus sur les XP. Antivirus Trend-Micro tenu à jour aux demi-heures sur tous les autres ordinateurs de l'entreprise.

Constat #3: Quelques PC d'utilisateurs infectés par le même virus ont été déconnectés du réseau, le temps de l'enquête.

Constat #4: Aucun serveur infecté, y compris ceux de la DMZ.

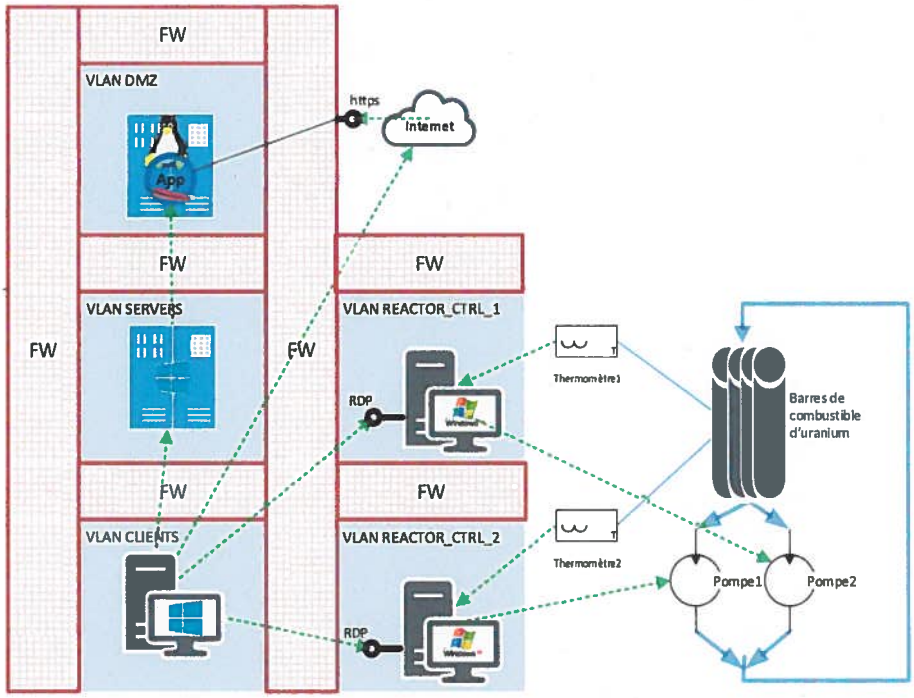


Figure 3: Architecture informatique du contrôle de refroidissement du cœur du réacteur nucléaire. Tous les circuits critiques sont dédoublés. Les ordinateurs de contrôle sont munis de Windows XP SP1. Un VLAN différent a été prévu pour ces ordinateurs et aucun accès à d'autre VLAN ou l'Internet n'est possible à partir de ces ordinateurs. Les flèches pointillées représentent les communications initiées permises par le Pare-Feu.

4.1 Quelles sont les précautions à prendre avant l'enquête? (*5pts*)

4.2 Quelles sont les étapes d'enquête? (*5pts*)

4.3 Quelles sont vos recommandations préliminaires pour éviter que la situation ne se reproduise avant la fin de l'enquête? (*5pts*)

4.4 Quelles sont les causes possible de cet incident à explorer selon vous? (*10pts*)
