UNIVERSITÉ DE SHERBROOKE

Université de Sherbrooke

Département d'informatique

IFT 606

Sécurité et cryptographie

Chargés de cours :

Marc Verreault

Mohammed Ouenzar

Examen périodique

Samedi 23 avril 2016, 9 h à 12 h

Défense, architecture et enquêtes

Consignes :

- Répondez directement sur le questionnaire;
- Inscrivez votre nom et matricule sur la première page;
- Cet examen comprend sept (7) questions réparties sur douze (12) pages et trois (3) pages d'annexes;
- Assurez-vous que toutes les questions s'y retrouvent;
- Seule une page de format 8½ x 14 est permise. Aucune autre documentation n'est permise;
- L'évaluation compte pour 35% de la note finale.

Nom : _____ Prénom : _____

Signature : _____ Matricule : _____

UNIVERSITÉ DE
SHERBROOKE

Question 1 : Défendre avec discernement *20 pts*

Vous êtes nouvellement embauché(e) à titre de responsable de la sécurité informatique et votre premier mandat consiste à déterminer cinq (5) mesures de défense «court-terme».

=> Utilisez les tableaux «scores» et SANS TOP-20 de l'annexe de l'examen.

Voici une description sommaire de votre organisation.

Sa mission est la fabrication et le développement de cosmétiques. Les trois principaux constats de sécurité rapportés lors d'un récent audit de sécurité réalisé par une firme externe sont :

1) Il n'y a pas de mises à jour des systèmes d'exploitation, entraînant des vulnérabilités des serveurs et postes de travail;
2) Les pare-feu sont configurés de manière trop permissive : il n'y a pas de rectriction d'accès Internet pour les utilisateurs et les serveurs;
3) L'équipe qui s'occupe de la sécurité des systèmes informatiques est en mode réactif et ne pose pas suffisamment d'actions préventives.

Au cours de la dernière année, les principaux incidents de sécurité ont été :

1) Cryptovirus introduits par les navigateurs WEB (à 10 reprises);
2) Attaque réussie du site WEB transactionnel ayant occasionné une perte due à l'indisponibilité du site transactionnel durant 24h;

Votre nouvelle entreprise est en croissance. On prévoit doubler le chiffre d'affaires dans la prochaine année. Votre budget n'est pas en enjeu pour mettre en place vos cinq (5) mesures. Le pare-feu a déjà la capacité adéquate. Il a les fonctionalités requises mais n'est pas configuré adéquatement.

1.1) Énumérez les mesures que vous proposez.

1.2) Expliquez chacune de ces mesures.

Question 2 : Défendre contre le déni de services *10 pts*

Voici six mesures de prévention du déni de service. Choisissez deux (2) mesures parmi elles et expliquez comment elles préviennent les attaques de déni de service.

1) Bloquer les protocoles ICMP et UDP;
2) Mettre en fonction le filtrage «ingress» et «egress» au Pare-feu;
3) Bloquer/désactiver la diffusion IP dirigée (*directed IP broadcasts*);
4) Configurer les limites de débit d'utilisation réseau;
5) Configurer l'authentification des équipements pour les échanges de tables de routage entre les commutateurs réseaux;
6) Implémenter des «sink-holes».

Question 3 : Défendre Microsoft Windows *10 pts*

Microsoft Windows est un système d'exploitation répendu et donc une cible de choix d'attaques. Donnez deux (2) mesures de défense contre l'énumération Windows.

Question 4 : Défense - Centrale nucléaire Irakienne *10 pts*

Vous êtes responsable de la sécurité informatique de l'unité de production de plutonium destiné au développement de l'arme atomique. Parmi les **méthodes de confinement** suivantes, votre équipe a par le passé choisi la sécurité physique. Discutez des avantages et inconvénients du confinement par isolement physique.

1) Confinement par isolement physique;
2) Confinement par virtualisation;
3) Confinement par interposition des appels systèmes.

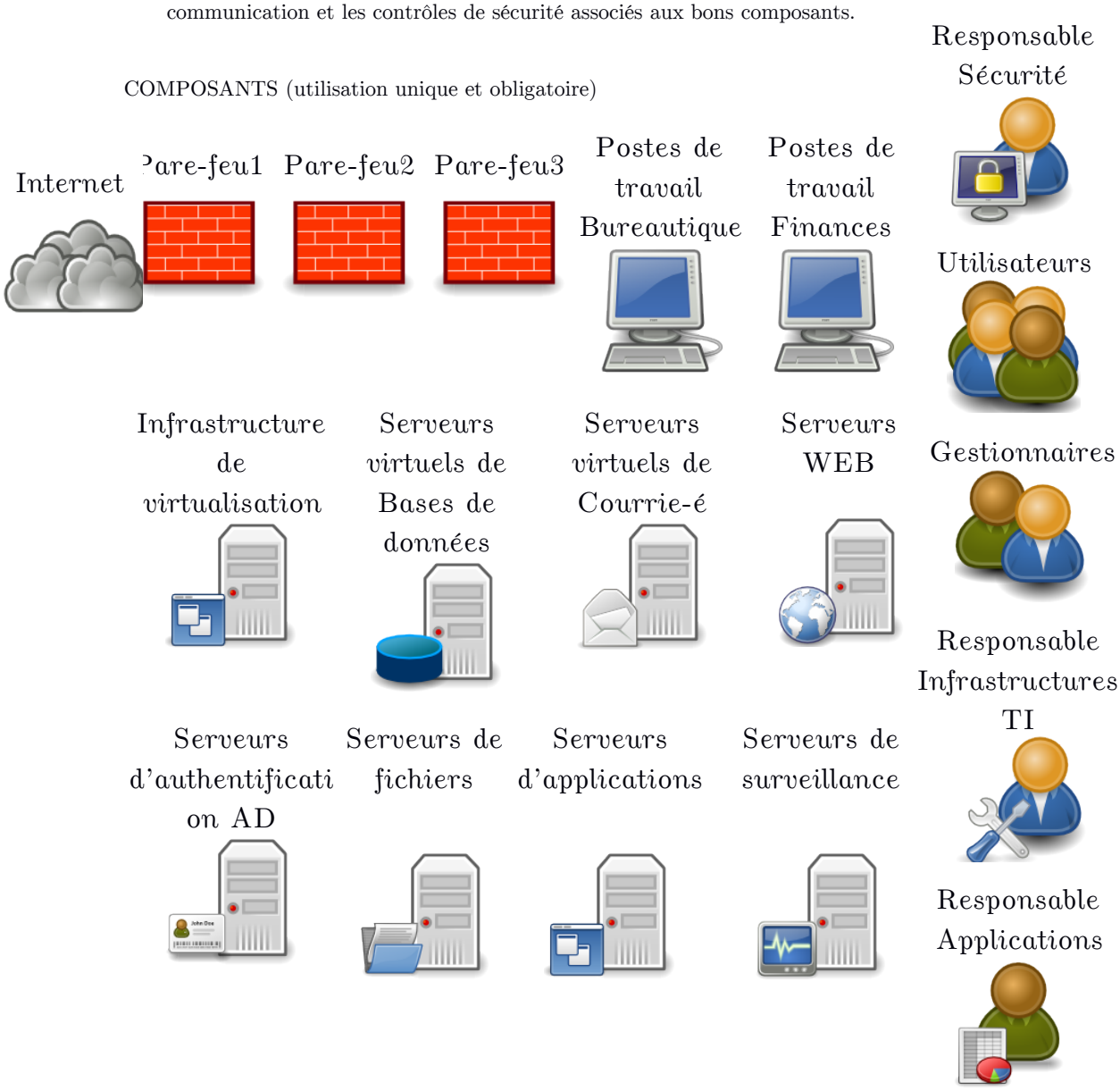
Question 5 : Défense : avantages de la virtualisation *15 pts*

Donnez trois (3) avantages et un (1) inconvénient de la virtualisation en termes de sécurité. Expliquez chacuns de ces avantages et de l'inconvénient.

Question 6 : Architecture : Fais moi un dessin *20 pts*

Dessinez une ***architecture de sécurité*** en utilisant les composants et contrôles ci-dessous de manière appropriée. Utilisez tous les composants. Les utiliser une seule fois. Vous pouvez utiliser les contrôles de sécurité zéro, une ou plus d'une fois. Utilisez une représentation de l'architecture technologique pour dessiner l'architecture de sécurité : dessinez les liens de communication et les contrôles de sécurité associés aux bons composants.

COMPOSANTS (utilisation unique et obligatoire)



CONTRÔLES DE SÉCURITÉ (utilisation multiple possible. Pas obligé de tous les utiliser)

AC-06	Accès et privilège minimal	**CP-02**	Plan de secours et d'urgence
AT-01	Sensibilisation à la sécurité	**IA-01**	Identification et authentification
AU-06	Revue des journaux, analyse et reporting	**SC-07**	Protection de la périphérie
AU-11	Conservation des journaux	**SC-08**	Confidentialité et intégrité des communications
CA-02	Audits et vérifications de sécurité	**SI-03**	Protection contre le code malicieux
CM-02	Configurations de base	**SI-04**	Surveillance des systèmes d'information
PE-01	Protection physique	**SI-08**	Protection contre le polluriel

Notes et remarques :

ARCHITECTURE DE SÉCURITÉ (votre réponse)

Question 7 : Enquête : ça sent pas bon... *15 pts*

Proposez un plan d'actions et les outils d'enquête, suite à l'incident décrit ci-dessous survenu dans une entreprise de transformation de poisson.

Date	Événement
1 avril : 10h30	Panne du contrôleur d'ensachage.
1 avril : 11h07	Découverte sur le contrôleur d'un service WEB contenant un site d'hameçonage actif.
1 avril : 12h30	Constat par l'administrateur réseau d'un pont réseau entre le serveur de la production et une adresse IP d'un service public de VPN chinois.
2 avril : 09h48	L'odeur de cette attaque ayant monté au nez de la direction, ces derniers font appel à vous pour savoir quoi faire.

PLAN D'ACTIONS

OUTILS D'ENQUÊTES

ANNEXE 1) Tableau des scores

D = Detect S = Stop		ATTAQUE Classe	Lecture					Manipulate			Spoof						Flood					Redirect				Composite			
		Sous-classe	Reconnaissance						Application manipulation				Transport Spoofing							L2 redirection									
Technology Class	Technology	Élément	Data Scavenging	Probe/ scan	War dialing	Sniffer	Direct access	Network manipulation	Buffer overflow	Web Application	MAC Spoofing	IP Spoofing	UDP Spoofing	TCP Spofing	Identity Spoofing	Rogue Devices	MAC flooding	Smurf	Distributed Denial of Service (DDoS)	TCP SYN Flood	Application flooding	ARP redirection / spoofing	STP Redirection	IP Redirection	Transport Redirection	Man-in-the-Middle (MITM)	Virus Worm/ Trojan Horse	Rootkit	Remote control software
		Overall Score																											
Identity	OTP	63					S								S														
	RADIUS/TACACS+	61					S								D														
	Reusable passwords	59					S								D														
	Smart Cards	55					S								S														
	PKI	54					S								S														
	Biometrics	52					S								S														
Hosts and App	Host AV	66																									S		S
	FS Check	61							D	D																	D	D	
	HIDS	61		D			D		D	D										D					D				D
	Host Firewalls	51		D			S																						S
Network FW	Stateful FW	89					S	S				S						D	D	S									
	Router with ACL	80					S	S				S						D	D					S					
Content	e-mail filtering	69																									S		S
	Web filtering	53					S																				S		
	Proxy server	43					S																						
NIDS	Signature-based NIDS	68		D				D	D	D		D						D	D	D		D					D		D
	Anomaly-based NIDS	51																D	D	D							D		
Crypto	Network Crypto	96				S	S					S			S											S			
	FS Crypto	91					S								S													S	S
	L2 Crypto	91				S	S				S				S											S			
	L5-L7 Crypto	88				S	S								S											S			
Hardening	Network device Hardening	44		S			S											S											
	OS Hardening	74		D			S		S																S			S	S
	Application Hardening	89		D			S		S	S															S			S	S
	Rogue Device Detection	44			S											S										S			
L2 Best practices	Physical Security	30			S		S																						
	L2 Control protocol BPs	30				S																	S						
	Port security	44				S					S						S												
	VLAN Hopping BPs	15					S																						
	ARP BPs	44				S																S				S			
	DHCP BPs	44				S																				S			
	Private VLANs	44				S	S															S							
Layer 3 BP	Role-Based Subnatting	15					S																						
	Ingress/Egress Filtering	74										S	S	S					S	S									
	Unicast RPF	74										S	S	S					S	S									
	ICMP BPs	15		S																									
	Routing protocol Auth	44					S									S								S					
DoS BPs	DDoS Eps	30																S	S								D		
	TCP SYN BPs	15																		S									

ANNEXE 2 : Tableau SANS TOP-20 mesures de sécurité

SANS Top 20 Critical Security Controls 2014

1	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
2	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3	Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
4	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
5	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
6	Manage the security lifecycle of all in--house developed and acquired software in order to prevent, detect, and correct security weaknesses.
7	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.
8	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
9	For all functional roles in the organization (prioritizing those mission--critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.
10	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
11	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

	SANS Top 20 Critical Security Controls 2014
12	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
13	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security--damaging data.
14	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.
15	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
16	Actively manage the life--cycle of system and application accounts – their creation, use, dormancy, deletion -- in order to minimize opportunities for attackers to leverage them.
17	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
18	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
19	Make security an inherent attribute of the enterprise by specifying, designing, and building--in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.
20	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.