Descriptif Technique

MÉTIER N°54
CYBERSECURITE

Soumis par :
Samy SCANNA - Expert WorldSkills France

SOMMAIRE

1. NOM ET DESCRIPTION DU MÉTIER

Le nom du métier est « Cybersécurité »

Description du métier :

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) définit la cybersécurité ainsi :
« Etat recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données ».

Il existe différents métiers dans le domaine de la cybersécurité, cependant chacun de ces métiers nécessite de s'approprier un socle de connaissances théoriques et pratique dans les domaines de l'administration des systèmes et réseaux, en développement applicatif, en gestion des bases de données.

On distinguera en particulier :

- **Les métiers d'analyste** : Agissant généralement dans un SOC (Security Office Center), ces acteurs ont pour principales missions de détecter tout évènement anormal dans le système d'information, le qualifier et y remédier
- **Les métiers d'auditeur en sécurité** : Souvent appelés pentesteurs, ces acteurs ont des compétences offensives et leurs principales missions ont pour objectif de tester la robustesse d'un système d'information aux tentatives d'intrusion et préconiser des solutions adéquates.
- **Les métiers de l'informatique légale :** Ce domaine, souvent intitulé « forensic » demande la mise en œuvre de protocoles d'investigation en phase avec la législation, et ont pour objet d'apporter des preuves numériques dans le cadre d'enquêtes judiciaires, ou internes à l'entreprise.
- Enfin, la mise en œuvre de politiques de sécurité dans l'entreprise est encadrée par des préconisations de l'ANSII, des normes ISO, leur mise en œuvre et application doit respecter la législation du pays dans lequel exerce une entreprise,

Documents complémentaires

Le descriptif technique ne contient que des informations relatives au métier. Il doit donc être utilisé en association avec le règlement de la WorldSkills Competition.

2. CONNAISSANCES ET PORTÉE DU TRAVAIL

Le Concours est une démonstration et une évaluation des compétences associées avec le métier en question. Le sujet d'épreuve est uniquement composé de travaux pratiques.

Compétences spécifiques

Liste des compétences spécifiques associées au métier :

- Sécurisation des composants actifs d'un réseau local (ex : utilisation de protocoles de communication sécurisés, désactivation des protocoles de découverte, sécurisation des mécanismes principaux des réseaux locaux dont ARP, DHCP)
- Mise en œuvre de tunnels VPN respectant les standards de sécurité modernes
- Sécurisation de services applicatifs
- Sécurisation de code applicatif (principalement PHP, Javascript, Java, Python, C)
- Sécurisation SQL (échanges, stockage)
- Scripting (Python, Bash, PowerShell)
- Connaitre et savoir situer un incident dans la Cyber Kill Chain
- Exploitation de logs (y compris maitrise des expressions régulières)
- Mise en œuvre et exploitation de SIEM (Splunk) ou de NSM (Security Onion)
- Sécurisation des systèmes d'exploitation Windows et GNU/Linux (recommandé : CentOS)
- Installation d'IDS/IPS (Snort/Suricata, NGFW: Palo Alto, Fortinet)
- Mise en place de sondes de collecte de données (port mirroring, TAP, syslog, ipfix)
- Mise en place de systèmes d'équilibrage de charge
- Mise en œuvre de WAF (pare feu applicatifs)
- Techniques offensives (Enumération active/passive, fingerprinting, recherche de vulnérabilité, exploitation, élévation de droits, buffer overflow, exfiltration de données)
- Connaissance des langages PHP, Javascript, Java, C, Python
- Utilisation de débugger et outils de reverse engineering (GDB, Immunity Debugger, IDA Pro)
- Pratique courante des outils standards (Nmap, Metasploit,)
- Reverse Engineering
- Systèmes Cryptographiques

Connaissances théoriques

Les connaissances théoriques sont requises mais ne seront pas testées à proprement parler :
CCNA Routing and Switching
CCNA Sécurité
CCNA CyberOps
CEH
OSCP
Security +
Certifications RedHat
Développement php/javascript/java, assembleur, C
Scripting Bash, Powershell, Python

La connaissance des règles et règlements ne sera pas testée.

Travaux pratiques

Cette compétition consiste en une démonstration et une évaluation des compétences nécessaires aux divers métiers de la cybersécurité.
Les missions confiées consistent en des tâches pratiques à réaliser, les compétiteurs doivent être en particulier capable de :

- Appliquer des règles de sécurisation strictes sur un environnement Active Directory
- Appliquer des règles de sécurisation strictes sur les principaux services d'une entreprise (serveurs HTTP, FTP, DNS, DHCP, VPN, Messagerie)
- Installer, configurer et exploiter des autorités de certification internes
- Sécuriser les équipements actifs des réseaux locaux
- Installer des systèmes de collecte de logs
- Installer, paramétrer et sécuriser des SIEM ou NSM, les interconnecter aux systèmes de collecte de logs
- Tester la robustesse d'une infrastructure, d'un serveur ou service
- Auditer la sécurité d'un code applicatif, proposer des méthodes de sécurisation du code audité
- Trouver les indices de compromission d'un système, recréer le timeline d'une attaque
- Détecter en temps réel des attaques aux moyens d'appliances NGFW et SIEM/NSM, repousser ces attaques au début de la cyberkillchain, documenter les faits
- Effectuer la rétro ingénierie de logiciels potentiellement malveillants

3. LE SUJET D'ÉPREUVE

Format / structure du sujet d'épreuve

Module A : Déploiement et sécurisation d'infrastructures, une demi-journée (3h30). Pas d'accès internet.

La mise en œuvre de cette infrastructure suivra les recommandations de mise en œuvre et sécurisation des constructeurs Microsoft et Redhat.

Un effort particulier devra être fourni sur les thèmes suivants :

- Politiques de sécurité des sessions et mots de passe
- Protection des services fournis aux clients
- Mise en œuvre de politiques de sécurité sur les pares-feux
- Surveillance active des flux de données entre endpoints, serveurs et clients
- Mise en œuvre de tunnels VPN

Module B : Capture the flag, une demi-journée (3h30). Pas d'accès internet.

Ce module prend la forme d'un audit de sécurité (Red Team), dans lequel il sera évalué
- La capacité à énumérer les systèmes à auditer
- La capacité à mener à terme des attaques sur services web
- La capacité à mener des attaques sur des bases de données
- La capacité à mener des attaques sur des systèmes Windows et GNU/Linux
- La capacité à élever les droits sur une machine compromise
- La capacité à traiter des problématiques de chiffrement et de stéganographie

Module C : Incident/Response, Forensic et sécurité applicative, une journée (7 heures). Pas d'accès internet.

Suite à compromission d'un ou plusieurs équipements, il est demandé d'investiguer : Analyser les méthodes employées par les attaquants, trouver les vulnérabilités exploitées, sécuriser le code incriminé, soumettre un rapport d'incident, nettoyer tout malware trouvé, restaurer les systèmes en état de fonctionnement optimal. Une partie portera sur de la revue de code dont l'objectif est d'identifier les parties vulnérables, expliquer les vulnérabilités et proposer un correctif

Module D : Cyberdéfense, une demi-journée, speed-module (3h30). Pas d'accès internet.

Ce module prend la forme d'un service de cyberdéfense (blue team), dans lequel il sera évalué à l'aide d'un générateur de trafic, d'une Appliance NGFW et d'un SIEM ou NSM la capacité de l'équipe à détecter et bloquer les types d'attaques suivantes :
- Attaques par reconnaissance
- Exploitation par malwares
- Phishing
- Botnet
- Exfiltration de données

Distribution/circulation du sujet d'épreuve

- **Le sujet du module A** sera diffusé 90 jours avant le début de l'épreuve, une modification d'environ 30 pourcent du sujet est à prévoir (retrait et ajout de certaines fonctionnalités).
- **Il n'est pas prévu de diffusion anticipée pour le module C.**
- **En préparation du module B**, plusieurs machines vulnérables seront recommandées 90 jours avant l'épreuve, la ou les machines de test préparées pour l'épreuve ne seront pas divulguées avant l'épreuve.
- **En préparation du module D**, les candidats doivent être en mesure de mettre en œuvre Splunk, Security Onion, et connaitre l'administration des NGFW Palo Alto. Un sujet de préparation sera proposé 90 jours avant l'épreuve, il s'agira bien d'un sujet d'entrainement : des traces PCAP seront proposées permettant aux candidats de s'entrainer à la détection d'intrusion.

4. NOTATION

Critères d'évaluation

SECTION	CRITERE	NOTE		
		Jugement (si applicable)	**Objectif**	**Total**
A	Déploiement et sécurisation		20	**20**
B	Incident/Response, Ferensic, Sécurisation de code	15	25	**40**
C	Red Team		20	**20**
D	Blue Team		20	**20**
	Total =		**100**	**100**

Spécification d'évaluation du métier

Certaines parties de la notation (notamment module B) sont des jugements subjectifs, notamment dans la qualité de la sécurisation du code proposée. Les notations subjectives seront réalisées par 4 jurés.
Les notations objectives correspondent à des critères mesurables (activité réalisée et fonctionnelle, ou non), et seront évaluées par groupe de 3 jurés.

5. EXIGENCES DE SÉCURITÉ LIÉES AU MÉTIER

Aucune exigence particulière n'est imposée pour ce métier.

6. ÉQUIPEMENTS ET MATERIAUX

Liste d'infrastructures

La liste des infrastructures reprend tous les équipements, matériaux et installations mis à disposition des compétiteurs sur les espaces de concours.

Matériaux, équipements et outils que les compétiteurs apporteront dans leur caisse à outils

Aucune caisse à outil n'est nécessaire pour ce métier.

Matériaux et équipements interdits sur l'espace de concours

Aucun système de communication numérique synchrone ou asynchrone n'est autorisé durant la compétition. Exemple : téléphones, ordinateurs, objet connecté).
Aucun appareil électronique appartenant au candidat ne sera accepté (exception ; matériel nécessaire pour les personnes en situation de handicap, dont la demande devra être produite en amont par le candidat).