REPUBLIQUE DU CAMEROUN

Paix - Travail - Patrie

MINISTERE DES POSTES ET TELECOMMUNICATIONS

REPUBLIC OF CAMEROON

Peace - Work - Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATION

RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL POUR LA REALISATION DE LA MISSION DE VEILLE SECURITAIRE.

MARCHE N° 00000040/M//MPT/SG/DAG/2021 DU 15 OCTOBRE 2021 PASSE APRES APPEL D'OFFRES NATIONAL RESTREINT N°00000025/AONR/MPT/CIPM/2021 DU 17 AOUT 2021 POUR LE RECRUTEMENT D'UN CABINET OU BUREAU D'ETUDES EN VUE DU RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL POUR LA REALISATION DE LA MISSION DE VEILLE SECURITAIRE

RAPPORT DE LA FORMATION SUR CPENT

Aout 2022

RAPPORT DE LA FORMATION SUR CPENT

LE PRESENT DOCUMENT EST LE RAPPORT DE LA FORMATION SUR LE MODULE CPENT DANS LE CADRE DU MARCHE N° 00000040/M//MPT/SG/DAG/2021 DU 15 OCTOBRE 2021 PASSE APRES APPEL D'OFFRES NATIONAL RESTREINT N°00000025/AONR/MPT/CIPM/2021 DU 17 AOUT 2021 POUR LE RECRUTEMENT D'UN CABINET OU BUREAU D'ETUDES EN VUE DU RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL POUR LA REALISATION DE LA MISSION DE VEILLE SECURITAIRE

SOMMAIRE

1. AVANT-PROPOS

Le présent document est confidentiel et sa confidentialité consiste à :

- La non divulgation des informations de configurations et paramétrages auprès de tierce partie ;
- La non reproduction des informations considérées confidentielles, sauf accord du Ministère des Postes et Télécommunications ;
- Les savoir-faire y contenus ne doivent profiter qu'au Ministère des Postes et Télécommunications ;
- Considérer toutes les informations déclarées Confidentielles.

2. Introduction et contexte

2.1. Contexte

Le CIRT est une structure de l'ANTIC constituée de seize (16) personnels chargés au quotidien de la prévention et de la réponse aux actes cybercriminels au Cameroun. Afin de remplir convenablement ses missions, le CIRT a besoin de personnels compétents dans différents domaines de la cybersécurité. A cet effet, le renforcement des capacités est une activité continue au sein du CIRT et permet de maintenir les personnels à la hauteur des enjeux auxquels ils font face au quotidien.

A travers ce projet, il est question d'améliorer les capacités des personnels au cours dans les domaines suivants :

- Ethical Hacking ;
- Les investigations numériques ;
- L'analyse des programmes malveillants ;
- La sécurité des infrastructures critiques ;
- La protection des postes clients ;
- La collecte des informations à travers les outils OSINT et le Dark web ;
- La protection des infrastructures critiques.

2.2. Objet du projet

L'objectif global de ce projet est de renforcer les capacités des personnels du CIRT afin de leur permettre de mieux réaliser les missions de veille de sécuritaire au sein de l'ANTIC.

Les objectifs spécifiques de ce projet sont les suivants :

- Permettre aux personnels du CIRT de mieux comprendre les techniques utilisées par les hackers, les risques de sécurité des systèmes d'information et les différentes mesures de sécurité existantes.
- Renforcer les capacités des personnels du CIRT en matière de collecte et d'analyse des preuves numériques sur les appareils mobiles, les supports de stockage, les mémoires vives, etc.;
- Permettre au CIRT de gérer les risques de sécurité afférents aux infrastructures critiques et aux systèmes de contrôle industriels ;
- Permettre aux personnels du CIRT de comprendre le fonctionnement du Dark web et d'être capable d'utiliser les outils OSINT pour la collecte d'informations spécifiques sur Internet ;

- Permettre aux personnels du CIRT d'analyser et comprendre le fonctionnement des programmes malveillants ;
- Permettre aux personnels du CIRT de maitriser la sécurisation des postes clients et des différents services qui s'y exécutent.

2.3. Consistance des prestations

Les prestations portent sur l'organisation de formation certifiante. Il s'agira donc concrètement de former les participants aux contenus en rapport avec le piratage éthique, l'investigation numérique, le test d'intrusion, la sécurisation des postes de travail, etc.

Chaque phase de cette formation (quatre au total) sera sanctionnée par un examen de certification pour évaluer l'assimilation et la mise en pratique des concepts appris.

Il s'agit des formations suivantes :

- Certified Ethical Hacker (CEH);
- Computer Hacking Forensic Investigator (CHFI);
- Certified Penetration Testing Professional (CPENT);
- Certified Secure Computer User (CSCU).

Le présent document constitue le rapport d'exécution de la formation sur CPENT.

3. Objectifs de la formation

3.1. Objectif général

L'objectif de cette formation est d'effectuer un test d'intrusion efficace dans un environnement réseau d'entreprise qui doit être attaqué, exploité, éludé et défendu.

3.2. Objectifs spécifiques

Les participants à la formation sont désormais capables de :

- Exécuter des tests d'intrusion pour déterminer les vulnérabilités et calculer divers risques de sécurité;
- Étudiez les résultats des tests d'intrusion qui aident à déterminer la probabilité d'exploitation et recommandent des actions de test post-intrusion;
- Étudiez les applications Web pour leurs vulnérabilités, enregistrez les protocoles de test de pénétration et estimez le risque d'exploitation;
- Évaluez les menaces pour auditer les contrôles de sécurité pour les risques et les réseaux de l'Internet des objets (IoT) et de la technologie opérationnelle (OT) ;
- Examinez les réseaux sans fil pour leurs vulnérabilités ;
- Exécutez la méthodologie de test d'intrusion complète pour évaluer la sécurité du mécanisme cloud d'une organisation.

4. Méthodologie choisie

Notre méthodologie a consisté en un cours intensif de cinq jours permettant aux participants d'apprendre comment effectuer une attaque, exploiter, esquiver et défendre.

Durant cette formation, les participants seront aussi en mesure faire des tests de pénétration dans un environnement de réseau d'entreprise qui devrait être exploité, défendu, attaqué et éludé.

L'agenda observé était le suivant :

Horaire	Activités	Animateurs	Horaire
08h00-10h00	Cours	Formateur	08h00-10h00
10h00-10h30	Pause-café	Formateur + Participants	10h00-10h30
10h30-12h30	Cours	Formateur	10h30-12h30
12h30-13h30	Pause déjeuné	Formateur + Participants	12h30-13h30
13h30-17h00	Cours	Formateur	13h30-17h00

5. Déroulement de la formation

La formation s'est déroulée sur une durée de 5 jours et a débuté le mardi 09 aout 2022 par l'installation des participants et le lancement officiel par les formateurs accompagnés de l'équipe projet de KIAMA SA.
Il a été rappelé les enjeux et les objectifs de la formation puis le matériel de formation a été distribué.
Le programme détaillé de la formation était le suivant :

Date	Modules dispensés
Jour 1 : 09 aout 2022	• Introduction aux tests d'intrusion • Portée et engagement des tests d'intrusion • Intelligence Open Source (OSINT)
Jour 2 : 10 aout 2022	• Tests d'intrusion d'ingénierie sociale • Test de pénétration du réseau – Externe • Test d'intrusion réseau - Interne
Jour 3 : 11 aout 2022	• Tests de pénétration du réseau – Périmètres périphériques • Test d'intrusion d'applications Web • Test d'intrusion sans fil
Jour 4 : 12 aout 2022	• Tests d'intrusion IoT • Tests d'intrusion OT/SCADA • Tests d'intrusion dans le cloud
Jour 5 : 13 aout 2022	• Analyse et exploitation binaires • Rédaction de rapports et actions de post-test

6. Domaines abordés

Les participants ont été entretenus sur les domaines suivants :

Domaine 1 : ATTAQUES AVANCÉES DE WINDOWS

Objectif principal : S'assurer que le candidat à la certification CPENT est en mesure d'abord accéder, puis utiliser PowerShell et tout autre moyen pour exécuter Silver et Gold Ticket et Kerberoasting. Les machines seront configurées avec des défenses en place, ce qui signifie que le candidat devra utiliser des techniques de contournement PowerShell et d'autres méthodes avancées pour marquer des points dans la zone.

Domaine 2 : Attaquer les systèmes IOT

Objectif principal : S'assurer que le candidat à la certification CPENT est en mesure de localiser les appareils IOT, puis à accéder au réseau. Une fois sur le réseau, le candidat devra identifier le micrologiciel de l'appareil IOT, l'extraire, puis le désosser.

Domaine 3 : Contournement d'un réseau filtré

Objectif principal : S'assurer que le candidat à la certification CPENT est en mesure d'identifier le filtrage de l'architecture puis tirer parti de ces connaissances pour accéder aux applications Web.

Domaine 4 : Pentesting de la technologie opérationnelle (OT)

Objectif principal : S'assurer que le candidat à la certification CPENT est en mesure de pénétrer du côté du réseau informatique et accéder au réseau OT. Une fois sur place, le candidat identifier l'automate programmable industriel (PLC) puis modifier les données pour impacter le réseau OT.

Domaine 5 : Analyse des bases de données et du réseau

Objectif principal : S'assurer que le candidat à la certification CPENT est en mesure de comprendre l'investigation des bases de données et son importance, comprendre l'investigation réseau.

Domaine 6 : Automatisation des attaques avec des scripts

Objectif principal : Le candidat à la certification CPENT devra se preparer aux techniques avancées de test d'intrusion et de script avec sept annexes d'auto-apprentissage : Test d'intrusion avec Ruby, Python, PowerShell, Perl, BASH, Fuzzing et Metasploit.

7. Conclusion

Le cabinet KIAMA SA, mandataire du groupement adjudicataire du marché de renforcement des capacités du personnel du MINPOSTEL pour la réalisation de la mission de veille sécuritaire a, dans cette étape réalisé le premier module portant sur la préparation à la certification CPENT. Il était question dans cette phase du marché, d'assurer la formation de cinq (05) personnels du MINPOSTEL et de l'ANTIC sur l'évaluation d'intrusion (PEN-TEST). Deux personnels de l'ANTIC n'ont pas pu prendre physiquement part à la formation. Nonobstant cela, la formation s'est déroulée normalement avec le personnel présent. Les participants présents ont bénéficié des attestations de fin de formation. L'ensemble des personnels conviés ont bénéficiés des packs iLeand de ECCOUNCIL contenant :

- Un an d'accès aux cours en ligne ;
- Six mois d'accès à l'environnement officiel de laboratoire en ligne d'EC-Council (i-Labs) ;
- Un voucher pour l'examen de certification d'EC-Council ;
- Un accès d'un an aux modules de formation d'experts d'EC-Council avec des présentations vidéo en continu pour un programme de formation complet qui offre les avantages d'une formation en classe à votre propre rythme ;
- Un accès au portail d'examen (https://www.eccexam.com) grâce à auquel chaque apprenant peut passer l'examen en ligne depuis le confort de sa maison ou de son bureau.

Le suivi d'après formation est effectif et se déroule dans le groupe whatsapp créé à cet effet.

Dans ce groupe, les apprenants remontent les difficultés éventuelles auxquelles ils font face et son coachés en prélude à leur examen.

ANNEXES

A1/ ATTESTATIONS DE PARTICIPATION

ATTESTATION DE FORMATION/ TRAINING CERTIFICATE

Le Comité d'Organisation remercie et félicite

The Organizing Committee thanks and congratulates

M. MBANGUE MOUKETE RAOUL MARC B.

Pour sa participation au renforcement des capacités pour la réalisation de la mission de veille sécuritaire qui s'est déroulée du 09 au 13 Aout 2022 à l'Ecole Nationale Supérieure Polytechnique – Yaoundé.

Il a été dans ce cadre préparé au passage de la certification **Certified Penetration Testing Professional (CPENT).**

For its participation in the capacity building for the realisation of the security watch mission which took place from 09 to 13 August 2022 at National Advanced School of Engineering of Yaoundé.

In this context, he was prepared for the **Certified Penetration Testing Professional (CPENT)** certification.

Responsable

KIAMA S.A.

YANNICK NGUEFACK

Formateur

NGUANGUE ARNAUD
Expert en Cybersécurité et Gestion des Risques

ATTESTATION DE FORMATION/ TRAINING CERTIFICATE

Le Comité d'Organisation remercie et félicite

The Organizing Committee thanks and congratulates

M. ZANZA SAKPEL FRANKLIN

Pour sa participation au renforcement des capacités pour la réalisation de la mission de veille sécuritaire qui s'est déroulée du 09 au 13 Aout 2022 à l'Ecole Nationale Supérieure Polytechnique – Yaoundé.

Il a été dans ce cadre préparé au passage de la certification **Certified Penetration Testing Professional (CPENT).**

For its participation in the capacity building for the realisation of the security watch mission which took place from 09 to 13 August 2022 at National Advanced School of Engineering of Yaoundé.

In this context, he was prepared for the **Certified Penetration Testing Professional (CPENT)** certification.

Responsable

KIAMA S.A. Direction Générale

NOUEFACK YANNICK

Formateur

NGUANGUE ARNAUD
Expert en Cybersécurité et Gestion des Risques

A2/ LISTES DE PRESENCE

KIAMA

Au cœur de l'innovation

KIAMA S.A. au capital de 40 000 000 de FCFA.
Bastos, en Face de l'ANOR, Rue Ambassade De Chine.
contact@kiama.cm www.kiama.cm
Tel : (237) 697 812 515 / 682 202 675
Fixe : (237) 222 209 043
BP : 15709 Yaoundé Cameroun

Yaoundé le, 09 Août 2022

FICHE DE PRESENCE A LA *FORMATION CPENT*

N°	NOMS ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE
01	NGUANGUE JOSEPH	Formateur	699947601	nguangujoseph2@gmail.com	
02	ZANZA SAKPEL FRANKLIN	Cadre/MINPOSTEL	697782408	sakpelfranck@gmail.com	
03	~~Mpessa Nanga Blaise~~	~~cadre Minpostel~~	~~674626051~~	~~Akeuacc@gmail.fr~~	
04	MBANGUE MOUKETE Raoul M. B.	CEA/MINPOSTEL	699325560	mbanguemouketeraoul@gmail.com	
05	WANKI MUKONG	CS/ANTIC	697017002	kwankiyi44@gmail.com	
06					
07					

KIAMA S.A. au capital de 40 000 000 de FCFA.
Bastos, en Face de l'ANOR, Rue Ambassade De Chine.
contact@kiama.cm www.kiama.cm
Tel : (237) 697 812 515 / 682 202 675
Fixe : (237) 222 209 043
BP : 15709 Yaoundé Cameroun

KIAMA

Au cœur de l'innovation

Yaoundé le, 10 Août 2021.

FICHE DE PRESENCE A LA *FORMATION CPENT*

N°	NOMS ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE
01	MBANGUE JOSEPH	FORMATEUR	699947601	mguangajoseph@gmail.com	
02	MBANGUE M Raoul	CEA A/DAG/MPT	699325560	mbangueraoul@gmail.com	
03	ZANZA Samuel Franklin	Cadre/DSR/Minpostel	697781408	samzafranck@gmail.com	
04					
05					
06					
07					

KIAMA

Au cœur de l'innovation

KIAMA S.A. au capital de 40 000 000 de FCFA.
Bastos, en Face de l'ANOR, Rue Ambassade De Chine.
contact@kiama.cm www.kiama.cm
Tel : (237) 697 812 515 / 682 202 675
Fixe : (237) 222 209 043
BP : 15709 Yaoundé Cameroun

Yaoundé le, 11 Août 2022

FICHE DE PRESENCE A LA *FORMATION CPENT*

N°	NOMS ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE
01	NGUANGUE JOSEPH	Formateur	699947601	nguangujoseph@gmail.com	
02	Zanza Sakpel Franklin	Coache/DSR/MPT	697789605	Sakpelfranck@gmail.com	
03	MBANGUE M. Raoul	CEA1/DAG/MPT	699325560	mbanguemoukete@gmail.com	
04	WANKI RUKONG	CS/CIRT	697097002	hallinki44@gmail.com	
05					
06					
07					

KIAMA

Au cœur de l'innovation

KIAMA S.A. au capital de 40 000 000 de FCFA.
Bastos, en Face de l'ANOR, Rue Ambassade De Chine.
contact@kiama.cm www.kiama.cm
Tel : (237) 697 812 515 / 682 202 675
Fixe : (237) 222 209 043
BP : 15709 Yaoundé Cameroun

Yaoundé le, 12 Août 2021.

FICHE DE PRESENCE A LA *FORMATION CPENT*

N°	NOMS ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE
01	NGUANGUE JOSEPH	Formateur	699947601	nguangjoseph@gmail.com	
02	Zouya Safael Franklin	Cadre/DSR/MPT	697789408	safaelfranck@gmail.com	
03	MBANGUE M. Raoul	CEA N/DAG/MPT	699 32 55 60	mbanguemouhite@gmail.com	
04					
05					
06					
07					

KIAMA

Au cœur de l'innovation

KIAMA S.A. au capital de 40 000 000 de FCFA.
Bastos, en Face de l'ANOR, Rue Ambassade De Chine.
contact@kiama.cm www.kiama.cm
Tel : (237) 697 812 515 / 682 202 675
Fixe : (237) 222 209 043
BP : 15709 Yaoundé Cameroun

Yaoundé le, 13 Août 2021.

FICHE DE PRESENCE A LA *FORMATION CPENT*

N°	NOMS ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE
01	NGUANGUE JOSEAH	Formateur	699947601	nguangujoseph@gmail.com	
02	Zanga Sakpel Franklin	Cadre/ASE/MPT	697789408	Sakpel Franckguai@	
03	MBANGUE M. Raoul	CEA/DAG/MPT	699325560	mbanguemaokete@gmail.com	
04					
05					
06					
07					

A3/ PHOTOS DE FAMILLE