Programme détaillé de formation du cours de Hacking Professionnel

HACKING PROFESSIONNEL ETHIQUE (CEH : Certified Ethical Hacking)

Module 1 : Préambule

a. Prérequis et Profil cible	**b.** Informations sur le formateur	**c.** Avantages de cette formation	**d.** Inconvénients de cette formation	**e.** C'est le Hacking Professionnel Ethique (Audit des S.I.)
f. Contenu et Durée de la formation	**g.** Examens aux certifications internationales	**h.** Mode de distribution des cours	**i.** La Loi Camerounaise sur la Cybercriminalité et la CyberSécurité	

Module 2 : Introduction au Hacking Professionnel Ethique

a. Comprendre le **Hacking Ethique**	**b.** Comprendre les termes associés au Hacking	**c.** Comprendre et appliquer la **Stéganographie** basique	**d.** **Types** et **catégories** de Hackers	**e.** Le Hacking éthique et le piratage informatique
f. Techniques **d'anonymat** sur Internet via les VPN	**g.** Les étapes d'une attaque de Hacking	**h.** Les types de tests **d'intrusions**	**i.** Technique d'extraction d'@mail d'une entreprise : **Email Hunting**	**j.** Hacking basique des caméras de surveillance

Module 3 : Installation et Configuration d'un Laboratoire de Hacking

a. Comprendre la **virtualisation**	**b.** Différence entre la **virtualisation** et la **simulation**	**c.** Acquisition d'un **Hyperviseur compatible** et des OS	**d.** Installation et configuration d'un Hyperviseur	**e.** Choix des OS Linux du Hacker
f. Installation des OS Windows	**g.** Installation des OS Linux du Hacker			

Module 4 : La Reconnaissance

a. L'importance de la Reconnaissance	**b.** Reconnaissance Active et Passive	**c.** Les outils de Reconnaissance	**d.** Techniques du **People Search**	**e.** Reconnaissance avec les services **WHOIS**
f. Reconnaissance avec **NetCraft**	**g.** Les outils : **host** et **dig**	**h.** Les outils : **dnsenum** et **dmitry**	**i.** **Email Harvesting** et **Email Hunting**	**j.** Le plus puissant : **Maltego**

Module 5 : Techniques de Scannage des Réseaux et Enumération

a. Comprendre le **scannage des réseaux** et le **scan informatique**	**b.** Analyse des **ports**, Analyse des **réseaux** et Analyse des **vulnérabilités**	**c.** La méthodologie de scannage	**d.** La communication en **3 étages** (TCP)	**e.** Comprendre le rôle d'un **pare-feu**
f. Technique de scan **Ping Sweep**	**g.** La base de données d'exploit **METASPLOIT**	**h.** Les commandes associés à **Nmap**	**i.** Scans local et distant avec **Nmap**	**j.** Scan distant avec **ZeNmap**

Module 6 : Le Cracking des Mots de Passe

a. Rappels importants et annonce des **bonus**	**b.** L'importance d'un Mot de passe dans un SI	**c.** Les **Types** de mots de passe	**d.** Caractéristiques d'un **bon** mot de passe	**e.** Comprendre les étapes du **System Hacking**
f. **L'escalade de privilèges**	**g.** Le Hachage et les fonctions de Hachage. **HascCalc**	**h.** Le Hachage **NTLM** des OS Windows	**i.** Les **techniques** et **outils** de cracking des mots de passe	**j.** Technique de **dumping** des mots de passe des OS Windows
k. Les **KeyLogger** et autres programmes **d'espionnage** des mots de passe	**l.** Cracking des mots de passe des sites et applications web	**m.** Cracking des mots de passe des OS Linux	**n.** Création et téléchargement des **dictionnaires de mots de passe**	**o.** Les techniques **non électroniques** de cracking des mots de passe

Module 7 : Hacking et Intrusions dans les Systèmes Informatiques

a. Comprendre la **pénétration directe** et la **pénétration à distance**	**b.** Les OS les plus fréquents dans les entreprises	**c.** Les **Flux de données alternatifs**	**d.** Utilisation de **MetaSploit** et **MsfConsole**	**e.** Pénétration directe sur les OS Windows XP, 2003 Server, 7, 8, 8.1, 10, 2012 Server
f. Pénétration directe sur les OS Linux	**g.** Téléchargement et Ajout de **nouveaux exploits** à MetaSploit	**h.** Les attaques de types **0-day**	**i.** Hacking des systèmes avec **Armitage**	**j.** Comprendre et appliquer la **redirection** des ports
k. Pénétration à distance des OS Windows et Linux par **Injection**	**l.** Pénétration à distance des OS Windows et Linux par 0-day	**m.** Techniques bonus : **Nuclear Rat, ez-sploit, Apocalypse**	**n.** Hacking **avancé** des caméras de surveillance	**o.** **Audit professionnel** d'un système informatique

Module 8 : Création des Logiciels malveillants (Cheval de Troie, Virus, Vers)

a. Comprendre le concept et exemple de **Malware**	**b.** Techniques de **propagation** des Malwares	**c.** Fonctionnement, création et utilisation d'un **Spyware** (Logiciel espion)	**d.** Relation entre **Malware** et **Spyware**	**e.** Système **d'espionnage** par intrusion informatique
f. Création et propagation des **Trojans**, **virus** et **vers**	**g.** Techniques de **Wrapping**	**h.** **Rootkit** et **Backdoor** avancés	**i.** Technique de **RansonWare** et **CryptoLocker**	**j.** **Détection** et **contremesures** des logiciels malveillants

Module 9 : Techniques de Reniflement des données

a. Comprendre le concept du **Sniffing**	**b.** Exemples d'informations sniffées	**c.** Fonctionnement d'un **Sniffer**	**d.** Types de Sniffing	**e.** Methodologie d'une attaque de sniffing
f. **Protocoles vulnérables** aux Sniffing	**g.** Idée derrière le Sniffing	**h.** **Prism**	**i.** Attaque par **inondation** de la table MAC	**j.** Attaque par **saturation** du serveur DHCP
k. Attaque par **empoisonnement ARP**	**l.** Attaque par **usurpation d'@ MAC**	**m.** Utilisation des meilleures Outils de Sniffing	Techniques de défense contre les attaques Sniffing	

Module 10 : L'Ingénierie Social (Hacking des Cerveaux)

a. Comprendre le concept de **l'Ingénierie Social**	**b.** Impacts, Facteurs et comportements vulnérables à l'IS	**c.** Types et Phases d'une attaque d'Ingénierie Social	**d.** Utilisation de **SET (Social Engineering Toolkit)**	**e.** Attaque de **Spoofing** et **Phishing**
f. Email and SMS **Spaming**	**g.** Mass Mailing, **Email Bombing**	**h.** Attaque **d'usurpation d'@mail**	**i.** Technique bonus : **Trity**	**j.** **Contremesures** du Social Engineering

Module 11 : Les Attaques de Dénis de services (DOS, DDOS, BotNet, Bot)

a. Comprendre le concept des **attaques DOS et DDOS**	**b.** Techniques d'attaques DOS et DDOS	**c.** Identification et utilisation des outils **pc** des attaques DOS et DDOS	**d.** Identifier et utilisation des outils **mobiles** des attaques DOS et DDOS	**e.** Compréhension et Création d'un **Bot**
f. Création et propagation d'un **Botnet**	**g.** Technique de **Zombification** des machines	**h.** **Bonus** : Télévision gratuite en ligne	**i.** **Bonus : Supervision réseau avec PRTG**	

Module 12 : Le Hijacking des Sessions				
a. Comprendre le concept du **Hijacking des Sessions**	b. Types d'attaques de **Hijacking des Sessions**	c. Hacking des **comptes web** sans username ni mot de passe	d. Prendre le **control total** d'un site web vulnérable au Hijacking	e. Les outils de Hijacking
f. **Protection** contre des attaques de Hijacking	g. **Bonus** : **Clonnage** des Serveurs Windows et Linux	h. **Bonus : Open Data Kit, PèFiaNoGhomabé et TontineSoft**	i. **Protocoles vulnérables** aux attaques de Hijacking	

Module 13 : Hacking et Intrusions dans les Serveurs Web				
a. Comprendre le fonctionnement d'un **Serveur Web**	b. Installation et configuration d'un serveur web (Laboratoire de **Web** Hacking)	c. Reconnaissance Web avec **Whois**, **HypeStat** et **YouGetSignal**	d. Reconnaissance Web avec **Netcraft**, **Nikto, idserve** et **W3af**	e. Techniques **d'aspiration** des sites et applications d'un serveur web
f. Prendre le control total d'un serveur web	g. **Audit professionnel** d'un Serveur web			

Module 14 : Hacking des Applications Web et Sites Web				
a. Quelques concepts des **Applications Web**	b. Installation, configuration et utilisation d'un application web (**Mutilidae**)	c. Failles et vulnérabilités des applications et sites web	d. Intrusion dans les bases de données des sites web et **extraction** des comptes users	e. Hacking des CMS (WordPress, Joomla, Drupal, …)
f. Attaque du **Cross-site scripting**	g. Création des programmes espion et destructif de Web Hacking	h. **Technique de scannage professionnel** d'une application web **et extraction de données**	i. **Audit professionnel** d'une Application web	j. **Outils de sécurité** pour les Application web

Module 15 : Les Injections SQL, Hacking des Bases de Données				
a. Quelques concepts des **Injections SQL** et des **Bases de données**	b. Types d'Injections SQL	c. Détection des applications et sites web **vulnérables** aux Injections SQL	d. Injections SQL sur les **formulaires de connexion**	e. **Extraction des identifiants et mots de passe** des users d'un site web

f. Injections SQL de type avancé, Les commandes **sqlmap**	**g.** Hacking des bases de données **MySQL**, **Oracle**, **PostGreSQL**	**h.** **Audit professionnel** d'une Base de données	**i.** **Attaque d'Extraction des numéros bancaires d'une base de données MYSQL**	**j.** **Technique de défense** contre les Injections SQL

16. Hacking des Réseaux sans fil (Wifi, Bluetooth, Brouillage Fréquences, Hotspot...)

a. Quelques concepts des **Réseaux sans fil**	**b.** Types de Chiffrement des Réseaux sans fil	**c.** Méthodologie de Hacking d'un réseau sans fil	**d.** Comprendre les attaques sur les réseaux sans fil	**e.** Installation et configuration d'un **Laboratoire de Hacking des réseaux sans fil**
f. Hacking des chiffrement **WEP, WPA, WPA2, WPA-PSK** des réseaux wifi	**g.** Hacking des **Hotspot avec portail captif** (Cyberlink, creolink, Necom, …)	**h.** **Brouillage des fréquences des réseaux sans fil (wifi, bluetooth, 4G, GSM, …)**	**i.** **Hacking des réseaux sans fil bluetooth**	

Module 17 : Hacking des téléphones mobiles (Appels, SMS, WhatsApp, …)

a. Installation et configuration d'un **émulateur-simulateur Android**	**b.** Installation du **programme mobile espion** sur les smartphones Android et Apple	**c.** **Ecoute** des appels téléphoniques et des SMS	**d.** **Tracking** des smartphones cibles via le GPS	**e.** Prise du control total du smartphone à distance
f. **Espionnage** d'images, vidéos, contacts	**g.** Espionnage des messages **whatsapp, facebook, insta; twitter**, …	**h.** **Bloquer le smartphone cible**	**i.** **Technique de déverrouillage d'un smartphone verrouillé par schéma ou mot de passe**	

Module 18 : Techniques de contournement des IDS, Pare-feu, et Antivirus

a. Comprendre le fonctionnement d'un **Système de Détection des Intrusions (SDI ou IDS)**	**b.** Comprendre les techniques et approches de contournement des SDI	**c.** Comprendre les **Pare-feu**	**d.** Technique de contournement des pare-feu	**e.** Comprendre le fonctionnement des **Antivirus**

f. Technique de contournement des antivirus				

Module 19 : Hacking du Nuage Informatique

a. Comprendre le fonctionnement du **Cloud Computing**	**b.** Comprendre et tester les attaques sur le nuage informatique	

Module 20 : Techniques de Cryptographie, Cryptanalyse et Décryptage

a. Comprendre les concepts de la **cryptographie** et les **algorithmes cryptographiques**	**b.** Cryptographie **Symétrique** et **Asymétrique** : RAS, AES, SSH, …	**c.** Techniques **d'encryptions des fichiers et répertoires**	**d.** Techniques d'encryptions des partitions logiques des disques	**e.** Chiffrement à **clé publique** et à **clé privée**
f. Technique de déchiffrement et de cryptanalyse				

Module 21 : Techniques d'obtention des Contrats d'Audit en Entreprise

a. Technique de Rédaction d'un bon CV d'auditeur de systèmes informatiques	**b.** Techniques de négociation du coût de l'audit d'un systèmes informatique	**c.** Exercer à l'étranger en occident	**d.** Exercer à l'étranger en Afrique hors du Cameroun	**e.** Exercer en tant que Employé dans une entreprise Camerounaise
f. Exercer en tant que Consultant pour une entreprise Camerounaise	**g.** Exercer en tant que Consultant pour un particulier	**h.** Exercer en tant que Employé pour une entreprise du domaine de la sécurité informatique	**i.** Exercer en tant que Employé pour une grande entreprise	**j.** Exercer pour la police judiciaire ou un corps similaire
k. Exercer dans un ministère ou Société d'Etat	**l.** Exercer en tant qu'enseignant en audit et Sécurité informatique	**m.** Que dire lors de l'entretien avec votre éventuel futur employeur ou partenaire	**n.** Lorsque les chefs d'entreprises sont conscients, inconscients ou avares	**o.** Lorsque les chefs d'entreprises sont conscients, inconscients ou avares

Module 22 : Astuces d'obtention des Stages et Emplois facilement

a. Technique de Rédaction d'un bon CV d'auditeur de systèmes informatiques	**b.** Techniques de négociation du coût de l'audit d'un systèmes informatique	**c.** Exercer à l'étranger en occident	**d.** Exercer à l'étranger en Afrique hors du Cameroun	**e.** Exercer en tant que Employé dans une entreprise Camerounaise

f. Exercer en tant que Consultant pour une entreprise Camerounaise	**g.** Exercer en tant que Consultant pour un particulier	**h.** Exercer en tant que Employé pour une entreprise du domaine de la sécurité informatique	**i.** Exercer en tant que Employé pour une grande entreprise	**j.** Exercer pour la police judiciaire ou un corps similaire

HACKING PROFESSIONNEL AVANCE

Module 1 : Hacking des Systèmes Bancaires

a. Quelques conseils sur **l'Ethique**	**b.** Identification des entreprises cibles	**c.** Conception d'un **Système d'Infiltration Bancaire** Avancé	**d.** Infiltration des Systèmes Bancaires par **Serveur 0-day**	**e.** Infiltration des Systèmes Bancaires par Rootkit, Shell et Trojan
f. Infiltration des Systèmes Bancaires par le **Web Hacking Avancé**	**g.** Infiltration des Systèmes Bancaires par **l'Ingénierie Social Avancé**	**h.** Hacking des comptes bancaires par **Espionnage Industriel**	**i.** Hacking des comptes bancaires par le **Account Hunting**	**j.** Hacking des comptes bancaires par **Usurpation des Numéros de Téléphone**
k. Extraction des données d'un serveur d'applications bancaires	**l.** Hacking des Banques par des relations humaines et des caméras de surveillance	**m.** Hacking des banques par le **Spoofing and Hacking Network Wi-Fi**	**n.** La **fouille** des poubelles bancaires	**o.** Hacking bancaire par Injections SQL

Module 2 : Hacking des Cartes Bancaires et Comptes PayPal

a. Quelques conseils sur **l'Ethique** et prérequis à avoir	**b.** Indentification des **Cibles** : Cartes Visa, Mastercard, Bleu, Prépayée, compte paypal, …, Banques et autres	**c.** Comprendre le **fonctionnement** des cartes bancaires et comptes paypal	**d.** Création et déploiement d'une **application standalone d'extraction en masse** des *numéros de cartes bancaires et compte Paypal*	**e.** Création et déploiement d'une **application web d'extraction en masse** des *numéros de cartes bancaires et compte Paypal*
f. Création et déploiement d'une **application Mobile d'extraction en masse**	**g.** Hacking d'une carte bancaire avec un **Stylo**	**h.** **Lecture du contenu de la puce** d'une carte bancaire	**i.** Hacking des cartes bancaires des **Black Hat** par **Ingénierie Social Avancé**	**j.** Hacking des **Lecteurs de carte bancaire intégrés aux ordinateurs**

des *numéros de cartes bancaires et compte Paypal*				
k. Carding Pro par le Sniffing, le Hijacking et Web Hacking Pro	**l. MTN CREDIT CRACKER**			

Module 3 : Hacking des Modems Huaïwei et QualComm				
a. Internet gratuit en fonction de votre équipement	**b.** Internet illimité peu importe votre F.A.I. ou réseau	**c. Augmentation de la bande passante** de votre connexion Internet	**d.** Hacking de modem et changement de son GUI, son OS, …	**e. Prise du control** du système informatique d'un modem à distance
f. Déconnecter un modem à distance sur le réseau du FAI	**g. Destruction** du système informatique d'un modem	**h. Techniques de détection des failles et vulnérabilités d'un modem**	**i. SIM cracking** des modems	**j.** Quelques attaques **Bonus**

Module 4 : Hacking des Grandes Entreprises (Projet de Black Hacking)				
a. Préparation physique et psychique	**b.** Sensibilisation et formation des forces de l'ordre et inspecteur de police	**c.** Travail de votre conscience, les risques et privations encourus,	**d. Préparation avant et après les attaques et intrusions de masse en entreprise**	**e.** Techniques avancées de diversion et d'anonymat
f. Les erreurs à ne pas commettre avant et après	**g.** Techniques de choix d'une cible d'évaluation	**h. Démarche minutieuse proprement dite dans le Hacking de masse des Grandes Entreprises**	**i.** Comment les Hackers Chapeaux noirs (Pirates) réfléchissent et agissent	

Module 5 : Cracking des Logiciels payants (L'ingénierie inverse)				
a. Comprendre le **reverse engineering**	**b.** Techniques de **contournement** des versions d'évaluation des logiciels payants	**c.** Comprendre les concepts de **crack**, **keygen** et **numéro de série**	**d.** Technique de **sauvegarde** des numéros de séries, mot de passe des logiciels d'un pc	**e.** Maitrise des prérequis, système de numération, Langage Assembleur, compilation
f. Technique de **création des cracks** de logiciels	**g.** Technique d'obtention des mot de passe	**h.** Technique d'obtention des numéro de série	**i.**	**j.**

Module 6 : Hacking des Comptes MobileMoney, OrangeMoney et EUMM				
a. Techniques d'obtention des **mots de passe** des comptes	**b.** Techniques de hacking des comptes par **espionnage mobile**	**c.** Technique de Hacking des comptes par le **SIM Cloning**	**d.** Techniques de hacking des comptes par **Ingénierie Social Avancé**	**e.** Techniques de hacking des comptes par **Usurpation d'identité du Service client**
f. Techniques de hacking des comptes par **injection de commande**	**g.** Techniques de hacking des comptes par **exploitation directe et à distance**			

Module 7 : Hacking des Réseaux de Téléphonie Mobile (GSM Hacking pro)				
h. Introduction à la Télécommunication	**i.** Introduction aux fréquences de communication	**j.** Brouillage des fréquences de communication	**k.** Définition et fonctionnement des réseaux 1G, 2G, 3G, …	**l.** Le Roaming et la carte SIM internationale
m. Hacking des Numéros de recharge avancé par Injection de Commandes GSM	**n.** Hacking des serveurs GSM et Extraction des numéros de recharge	**o.** Hacking des bases de données téléphoniques	**p.** Procédure d'audit d'un système GSM	**q.** Technique d'Usurpation des Numéros de téléphones
r. Contrôle de Puces électronique à distance	**s.** Techniques avancées d'Appel et de SMS gratuits	**t.** Hacking des crédits de communication	**u.** Technique de clonage des cartes SIM	**v.** Ecoute téléphonique fréquentielle
w. Ecoute téléphonique non fréquentielle	**x.** Ecoute téléphonique par la raisonance	**y.** Technique d'usurpation d'un opérateur de téléphonie	**z.** Technique d'Appel gratuit sans carte SIM	

Module 8 : Hacking des Chaînes de Télévisions et Fréquences Radios				
Module 9 : Hacking des Jeux de Hasard PariFoot, PremierBet, XBet, …				
a. L'application Par!Foo!W!nner par GroupeDeGénie	**b.** Technique d'optimisation des chances de gain	**c.** Hacking des sites de pari par Injection de commande	**d.** Hacking des sites de pari par Intrusion de masse	
SANS DOUTE LA MEILLEURE FORMATION ACTUELLE DE HACKING PRO				



Informations sur le Formateur

1. Hacker Professionnel *(White Hat)*
2. Expert en Sécurité Informatique
3. Ingénieur Système et Réseau
4. Génie Logiciel et Développement avancés
5. Open Data Kit *(Collecte de données via les smartphones)*
6. S.I.G et Système d'Information Sanitaire

Chaîne YouTube pour les vidéos Démo : F.K.S. GroupeDeGénie-Sarl

Contacts : support@groupedegenie.com // +237 662420795

Nom et Prénoms : FETCHEPING K. SHAMIR, *Fondateur GroupeDeGénie-Sarl*