MBIS
SOLUTIONS IT & TELECOM

DIGITAL FORENSIC

MBIS Algiers, ALGERIA , Zergoug Lot N°02
Hydra, Algiers, Algeria, 16016
www.mbis-inc.net
https://www.linkedin.com/company/mbis-inc/
+213 (0) 21 54 68 50
+213 (0) 21 54 68 59
+213 (0) 21 54 77 55
info@mbis-inc.net

MBIS
SOLUTIONS IT & TELECOM

DIGITAL FORENSIC :

La criminalistique numérique est l'application de méthodes scientifiques pour aider à préserver, récupérer et enquêter sur les preuves numériques en cas de cybercriminalité.

Ceux qui travaillent sur le terrain ont besoin d'une immense quantité de compétences et de connaissances pour assumer les responsabilités nécessaires.

Au cours de ce cours, vous serez informé des principes fondamentaux de la criminalistique numérique, y compris l'acquisition de données, Windows Forensics, Network Forensics et bien plus encore.

Conditions Préalables :

OS :
- très bonne connaissance des architectures OS Windows et Linux
- les librairies sous Windows et Linux
- Debugging d'application sous Windows et Linux

Langage de programmation :
- très bonne connaissance du langage C
- bonne connaissance du langage assembleur.
- bonne maîtrise Architecture Réseaux sécurisées, SOC SIEM.

• **DURÉE DU COURS:** 32 à 35 HEURES

www.mbis-inc.net
+213 (0) 21 54 68 50

MBIS
SOLUTIONS IT & TELECOM

Pourquoi choisir MBIS ?

MBIS est une société prestataire de service, sa mission est de fournir des solutions complètes dans la sécurité informatique et IT, les sciences forensics et la cybersécurité. MBIS est une référence dans les technologies forensics et cyber sécurité en Algérie pendant plus de 10 ans.

Nous effectuons des inspections dans le monde entier pour sélectionner les meilleures solutions pour nos clients, nous participons à des nombreux congrès et séminaires spécialisés en cyber sécurité et cyber-forensics.

Nos partenaires sont parmi les leaders dans les technologies forensics en monde entier. Nous travaillons ensemble pour fournir des solutions complètes et sur mesure pour nos clients.

Nous avons également une équipe dédiée d'ingénieurs qualifiés en informatiques et télécommunications, formés et certifiés dans la cyber-sécurité et cyber forensics, dans l'administration des systèmes et des réseaux.

MBIS offre une formation avancée sur la cybersécurité en :

1. Hacking Target Environment.
2. Hacking Network Infrastructure.
3. Hacking Web Application.
4. Hacking System Linux.
5. Hacking System Windows.
6. Digital Malware Forensics Investigation.

et plus : https://www.mbis-inc.net/formations-en-securite-it.html

Nous fournissons une formation professionnelle qui comprend des défis du monde réel.

Formation orientée %100 pratique.

www.mbis-inc.net
+213 (0) 21 54 68 50

MBIS
SOLUTIONS IT & TELECOM

Carrière dans le domaine de la sécurité informatique :

- Consultant senior en sécurité Testeur de pénétration.
- Agent d'analyste des incidents.
- Chef de la sécurité de l'information.
- Analyste de code logiciel.
- Hacker éthique.
- Contrôleur des risques.
- Architecte de sécurité.
- Développeur d'exploit.
- Analyste de la sécurité de l'information.
- Expert médico-légal numérique.
- Ingénieur sécurité.

Objectif de la Formation :

De nos jours, nous lisons de plus en plus d'article sur le net qui parlent des APT (menaces persistantes avancées) , des Malwares qui restent des années indétectables, sachant que aucun organisme au monde

N'échappe a ces APT, parfois même un pays entier est Paralysé. Tel que l'Estonie, des organismes qui ont les moyens de se protéger par les dernières technologies, comme les Banques, Les Institutions gouvernementales telles que NASA, institutions Militaires.

Une question qu'on doit se poser est comment ces APT arrivent elles à outrepasser tous les systèmes de détections et de préventions de sécurité Informatique qui existent ?

C'est ce que nous allons voir tout au long de cette formation, comment fonctionnent ces APT, leurs moyens de propagation, leur mode de furtivités et enfin quel sont les moyens a mettre en place pour les détecter et les éradiquer.

www.mbis-inc.net
+213 (0) 21 54 68 50

MBIS
SOLUTIONS IT & TELECOM

Déroulement de la Formation :

Cette formation est orientée 100 % technique, nous allons examiner certain APT qui ont fait des millions de victimes dans le monde tel que Stuxnet, Zeus, SpyEye, SilentBanker, CoreFlood, Laqma, Cridex, BlackEnergy, et plus encore.
Au premier lieu nous allons outrepasser les systèmes de détections et de préventions tels que Host IDS/IPS, Network IDS/IPS, Firewall.
Puis nous allons comprendre leurs Mode de propagation (Failles Applicatives, Zero Day), et comment fonctionne leur mode de furtivité.
Et enfin nous allons faire des investigations (statique, dynamique, analyse mémoire (post-attaque)) afin de déceler les toutes dépendances en terme fichiers , librairies afin de les éradiquer.

Course Overview :

Malware mode de fonctionnement :

- Trojan.
- Rootkit User et KERNEL LAND.

Analyse Statique des Malwares :

- Obfuscation.
- Anti Virus et mode de fonctionnement, ClamAV.

Analyse Dynamique des Malwares :

- SandBox et mode de fonctionnement.

Bypass Host IDS/IPS :

- Injection de Code Malveillant dans des Applications.
- Injection de Code Malveillant dans des Processus - PID.
- Persistance.
- Hooking Library Function.

Bypass Host IDS/IPS :

- TUNNELING & Data Exfiltration
- SHELLCODE Polymorphique.

Malware Forensics Investigation

www.mbis-inc.net
+213 (0) 21 54 68 50

MBIS
SOLUTIONS IT & TELECOM

Déroulement de la Formation :