



Vos contacts :
Marie-Jeanne ou Marjorie
au : 05 61 34 39 80

SEC06 – Analyse avancée de la sécurité

Objectifs	A l'issue de ce stage, vous serez capable de configurer des outils de monitoring ainsi que de répondre rapidement à une attaque
Public concerné	Responsables de la Sécurité des Systèmes d'information ou Responsables de l'exploitation des systèmes et réseaux .
Pré requis	Pour suivre ce stage, il est recommandé d'avoir suivi le cours SEC01 – Attaques et Contre-mesures ou d'avoir des connaissances équivalentes - Il est préférable de maîtriser les réseaux, pare feu, IDS, honeypot
Durée	5 jours

Contenu

Module 1 : Les bons comportements

- Comment réagir face à une mauvaise configuration
- Comment réagir face à une attaque

Module 2 : Les recherches internet

- Google
- Les outils

Module 3 : Analyses des paquets

- Analyse
 - o TCP
 - o UDP
 - o ICMP
- Sniffing
 - o Wireshark
 - o Tshark
- Wifi
 - o WEP
 - o WPA
 - o WPA2

Module 4 : Analyse par Nessus

- Scanning
- Enumération
- Détection de vulnérabilité

Module 5 : DMZ

- Les différentes DMZ
- La mise en place d'une DMZ

Module 6 : Les moyens de prévention

- Pare feu
 - o Statefull
 - o Stateless
 - o Proxy
- Honeypot
- IDS/IPS

Module 7 : Les outils

- Snort
 - o Implémentation et analyse
- Iptable
 - o Les règles à appliquer
- ISA
 - o La mise en place sur un réseau Microsoft
- ASA/Pix
 - o Mise en place sur un réseau Cisco

Module 8 : Analyse de logs

- Base SQL log
- Client VPN log
- DHCP log
- Analyse restreinte des logs

Module 9 : Les outils d'un test d'intrusion

- Metasploit
- Core impact
- Debugger