

Techniques de hacking et contre-mesures



La sécurité informatique se distingue par un besoin spécifique de précision et de pragmatisme. L'esprit de ce stage est bien de mettre de côté les discours généralistes pour entrer dans le vif du sujet : en face de chaque technique de hacking, proposer des remèdes concrets. Il permet donc d'obtenir des résultats palpables

Objectifs

- Comprendre les risques, évaluer leur portée
- Connaître les techniques de hacking, repérer les failles
- Identifier les mesures à adopter, engager des actions préventives et correctives
- Définir les priorités d'investissement en terme de sécurité

Public concerné

- Responsables sécurité des systèmes d'information (RSSI)
- Responsables de sites Web
- Les responsables Intranet et tout responsable informatique (DI, Responsables télécoms/réseaux...) en charge de la sécurité informatique ou désirant se tenir informé dans ce

Pré requis

- Avoir suivi les stages SR230 : "Soyez autonome avec TCP/IP", SR211 : "Mettre en oeuvre la sécurité réseaux" ou SR220 : "Concevoir et mettre en oeuvre la sécurité du système d'information" ou connaissances équivalentes

Une formation de 4 jours

Caractéristiques	Paris
Tarif : 2600 € HT par personne	15/12/2008
Numéro de formateur : 11753687675	09/03/2009
Nombre d'heures : 28	15/06/2009
Référence : SR225	05/10/2009
Contact : Patrick LE GOFF	14/12/2009
Telephone : 01.76.60.66.10	
Email : contact@kaptive.com	

Description des modules

num	Module
1	La sécurité au coeur des débats
Détails	<ul style="list-style-type: none"> - Évolution des systèmes d'information - Omniprésence d'Internet - Aggravation des risques - Statistiques sur l'évolution des malveillances - Sociétés victimes
2	Les forces en présence
Détails	<ul style="list-style-type: none"> - La position du hacker : intrusion dans un réseau, sur les ordinateurs, éviter les mécanismes de filtrage, profiter des «trous» de sécurité - Le rôle du RSSI : contrôler les défenses périmétriques, renforcer les défenses des ordinateurs, monitorer les éléments mis en place, faire tester par un tiers la sécurité
3	Les hackers
Détails	<ul style="list-style-type: none"> - Les différents types de hackers - Les grandes étapes d'un hacking (approche, analyse, attaque)
4	Les attaques
Détails	<ul style="list-style-type: none"> - Introduction aux différents types d'attaques - Le War Dialing - Le traçage réseaux (utilisation de traceroute) - Les reconnaissances (utilisation de DNS et WHOIS) - Les attaques réseaux (sniffing, spooling, man in the middle, TCP session Hijacking, dénis de service) - Les attaques systèmes (Buffer Overflow, les vulnérabilités système, les DoS système) - Les attaques applicatives (mauvaise configuration, source Disclosure, Unexpected Input) - La sécurité des messageries électroniques - La sécurité des technologies Web (ASP, Perl, PHP, Java, .Net)
5	Le détournement de moyens informatiques
Détails	<ul style="list-style-type: none"> - Spamming - Virus - Chevaux de Troie - Surfing abusif - Vol d'ordinateur portable - Fuite d'informations - Social Engineering
6	Comment se protéger efficacement ?
Détails	<ul style="list-style-type: none"> - Politique de sécurité - Gestion des mots de passe - Veille technologique - Choisir ses produits - Administrer sa sécurité - Tester sa sécurité - Que faire après un acte de malveillance ? - Faire appel à des spécialistes - Conclusion