Hacking et Sécurité - Niveau expert

Protéger étape par étape un système d'information

Présentiel ou en classe à distance

5 jours (35 h)

Prix inter : 4.050,00 € HT
Forfait intra : 12.290,00 € HT

Réf.: SE104



L'actualité nous le rappelle quasi quotidiennement, les intrusions dans des systèmes informatiques publics ou privés existent. Et bien souvent, les entreprises et organisations qui en sont victimes sont pointées du doigt pour n'avoir pas su correctement protéger leurs données. Si le risque 0 n'existe pas, il apparait presque évident qu'en éprouvant son SI régulièrement, les équipes en charge de garantir la sécurité peuvent être amenées à détecter de nouvelles failles ou menaces et ainsi mettre en oeuvre la correction ad' hoc... Durant cette formation très pratique qui consiste en une série d'ateliers ponctuée d'échanges, les participants auront à disposition un environnement technique complexe qu'ils pourront attaquer à loisir pour mieux le protéger par la suite, apprenant ainsi à le protéger un système de bout en bout.

A qui s'adresse cette formation ?

- Développeurs
- Administrateurs systèmes / réseaux
- Ingénieur sécurité
- Consultant sécurité

- Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou disposer des compétences équivalentes
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

Pendant

1 - Introduction

- Définition du hacking
- Panorama 2018/2019
- Référentiel de sécurité (ANSSI, ENISA, CLUSIF, Cybermalvaillance.gouv etc...)
- Les différents types de hackers
- Les différents types d'attaques
- Les différents outils utilisés par le hacker
- Le cycle de l'attaquant

2 - Le Hacking

- Scan de réseau/ports/versions

- Exploitation de CVE
- Élévation de privilège
- Mise en place d'une backdoor
- Récupération d'informations, création d'un dictionnaire + Bruteforce
- Payload msfvenom MITM
- Saut de VLAN (yersinia et/ou table overflow)

3 - Les piliers de la sécurité

- Confidentialité
- Intégrité
- Disponibilité
- Traçabilité

4 - Les grands principes de la sécurité

- IAAA
- Authentification
- Need to know
- Least Privilege
- Non répudiation
- Défense en profondeur

5 - La sécurité physique

- Notion de sécurité physique
- Mise en correspondance des notions avec les principes précédents

6 - Sécuriser le réseau

- La sécurité de la couche 2 : Port security, vLlan, Ssh, dhcp snooping, Defense contre arp MITM, Sécurité pour DTP,CDP,VTP,STP.
- La sécurité de la couche 3 : IPSec, routeur filtrant
- La sécurité de la couche 4 : Explication de la passerelle d'interconnexion de l'ANSSI, Travaux pratiques sur PFsense, explication des IDS/IPS , présentation de Snort, travaux pratiques sur Snort
- La sécurité de la couche 5 : Le proxy

7 - Sécuriser le système

- Hardenning sur Linux
- Hardenning sur Windows
- Mise en place d'HIDS

8 - Supervision de la sécurité

- Présentation SOC
- Présentation SIEM
- Présentation de ELK et Splunk
- Mise en place de ELK ou Splunk pour analyser les Logs

9 - Réponse à incident

- Rejouer les attaques
- Analyser les logs
- Utiliser WireShark



Les objectifs de la formation

- Savoir protéger son système d'information
- Comprendre comment sécuriser tous les aspects d'un SI : réseau, applicatifs et Web
- Acquérir les connaissances et compétences nécessaires pour détecter des failles et mettre en oeuvre des parades
- Savoir correctement réagir en cas d'attaque soudaine
- Être capable de mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Le passage en revue des principales techniques de défense et outils utilisés.
- L'utilisation d'outils d'analyse et d'automatisation des attaques.
- Une formation très pratique : l'essentiel de la formation portera sur des contre-mesures concrètes techniques que chacun peut mettre en oeuvre dans son établissement.
- L'apport de consultants experts en audits techniques des SI.
- 90% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Dates et villes 2027 - Référence SE104

Dernières places disponibles Session garantie

A distance

du 1 févr. au 5 févr.	du 30 août au 3 sept.
du 31 mai au 4 juin	du 13 déc. au 17 déc.

Paris

du 1 févr. au 5 févr.	du 30 août au 3 sept.
du 31 mai au 4 juin	du 13 déc. au 17 déc.