ENI Service

référence
T130-030

21h

La sécurité des réseaux TCP/IP

Mise à jour
16 octobre 2026

1800 € HT

Présentiel/distanciel

TOP FORMATION

La sécurité des réseaux TCP/IP

Objectifs pédagogiques

- Décrire les risques internes et externes liés à l'utilisation de l'Internet
- Décrire l'architecture réseau et les matériels/serveurs pour me connecter à Internet en sécurité
- Décrire les principes de signatures et chiffrement
- Protéger le réseau local
- Autoriser l'accès sécurisé au réseau aux utilisateurs nomades
- Préserver votre réseau des attaques
- Construire un Intranet utilisant Internet

Prérequis

Avoir suivi la formation T101-045 Théorie des réseaux locaux et protocole TCP/IP ou disposer de connaissances équivalentes, et maîtriser un système d'exploitation.

Public concerné

Equipes réseaux, systèmes, sécurité.

Programme détaillé

Pourquoi sécuriser votre réseau d'entreprise (2 heures)

- Les risques, les attaques
- La dissimulation et vols de mots de passe
- Les virus, la propagation par e-mail
- Le cheval de Troie
- La circulation des données dans l'entreprise
- D'où vient l'attaque : de l'extérieur ou de l'intérieur ?
- Quelques chiffres : estimations de coûts d'immobilisation

Les risques inhérents à TCP/IP et à l'Internet (3 heures)

- La circulation des données en clair
- La substitution des adresses IP (IP spoofing)
- Les attaques par IP, ICMP, TCP, UDP
- Les failles connues des applications FTP, SMTP, DNS
- Risques liés aux réseaux locaux sans fils (802.11)

Ouvrir son réseau d'entreprise à l'Internet (3 heures)

- La gestion des adresses privées / publiques
  - RFC 1918
  - Masquer son plan d'adressage privé
  - Les translations d'adresses N vers 1 ou N vers N
- Les solutions routeur filtrant
  - Filtrage sur paquets IP (adressage)
  - Filtrage sur segment de transport (ports applicatifs)
  - Translation d'adresse NAT
  - Les solutions Firewall
  - Fonctionnalités des Firewalls
  - Firewall à état
  - Firewall matériel vs Firewall logiciel
  - Les firewalls tout en un
- Les solutions serveur Proxy
  - Qu'est-ce qu'un Proxy
  - Qu'apporte un Proxy en termes de sécurité
  - Où positionner un Proxy ?
  - Complémentarité serveur Proxy/Firewall
- Les IDS/IPS
- DMZ
  - Pourquoi une DMZ ?
  - Comment créer une DMZ

Protéger les données de l'entreprise (3 heures)

- Confidentialité
- Signature
- Intégrité
- Non répudiation
- Infrastructure à clefs publiques (PKI)
- Exemple applicatif : SSL, EFS, IPSec etc.
- La cryptographie : jusqu'où peut-on aller en France ?

Protéger le réseau local (3 heures)

- Architecture (VLAN etc.)
- Sécurisation de postes de travail
- Sécurisation des serveurs
- Politique antivirale
- Chiffrement des données sensibles
- Sauvegarde
- Chiffrement des flux sensibles

Permettre l'accès à son réseau pour les utilisateurs nomades (3 heures)

- Accès via RTC ou Numéris : avantages et inconvénients
- Accès via GSM ou GPRS : avantages et inconvénients
- Sécurité de connexion
  - Call back
  - Authentification
  - CHAP
  - PAP
  - SecureID
- Les réseaux privés Virtuels (VPN)
  - Avantages et inconvénients
  - Techniques de VPN
    - Site à site
    - Nomade à site
    - Protocole PPTP
    - Protocole L2TP/IPSec
  - VPN SSL
    - Principe des VPN SSL
    - Avantages et limitations
- Application Web
- Application métier
- Accès à sa messagerie de façon sécurisé via Internet

Bâtir son Intranet en utilisant un réseau public (2 heures)

- La sécurité des informations transportées
- Routeurs ou Firewall
- Les solutions VPN du marché

Les sites majeurs de la sécurité (1 heure)

- CERT, ITPRC etc.

Qu'apporte IPV6 en matière de sécurité ? (1 heure)

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes, le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation