

Mis à jour le 08/10/2026

S'inscrire

Formation IPv6 Security Lab

2 jours (14 heures)

Présentation

IPv6 transforme profondément le fonctionnement des réseaux avec de nouveaux mécanismes d'adressage, d'autoconfiguration et de découverte. Ces évolutions introduisent également des surfaces d'attaque spécifiques qui doivent être maîtrisées pour sécuriser les infrastructures IPv6 et dual-stack.

Notre formation Sécurité IPv6 : attaques, défense et ateliers pratiques vous permettra d'identifier, reproduire et analyser les principales menaces affectant les environnements IPv6 afin de mettre en œuvre les protections adaptées.

Vous étudierez en particulier les risques liés à ICMPv6, Neighbor Discovery, Router Advertisement, SLAAC et DHCPv6. Vous apprendrez à reconnaître les scénarios de reconnaissance, spoofing, Rogue RA, flooding et détournement de trafic puis à appliquer les mécanismes de défense appropriés.

La formation aborde également les risques associés aux en-têtes d'extension, à la fragmentation, aux tunnels et aux environnements dual-stack. Vous apprendrez à construire des règles de filtrage adaptées à IPv6 et à vérifier la cohérence des politiques de sécurité entre IPv4 et IPv6.

Grâce à une approche fortement pratique, vous analyserez les flux avec Wireshark, exploiterez les logs et mécanismes de détection puis reproduirez des attaques dans un laboratoire isolé afin d'en comprendre les effets et de valider les contre-mesures.

À l'issue de cette formation, vous serez capable d'auditer, détecter et corriger les principales faiblesses d'une infrastructure IPv6 et de construire un Security Lab permettant de tester vos mécanismes de défense avant leur déploiement en production.

Objectifs

- Identifier les principales surfaces d'attaque IPv6
- Analyser les risques liés à ICMPv6, NDP, Router Advertisement, SLAAC et DHCPv6
- Reproduire et comprendre les attaques de reconnaissance, spoofing, Rogue RA et flooding
- Sécuriser les environnements dual-stack, les en-têtes d'extension et les mécanismes de transition
- Configurer les protections L2/L3 et les règles de firewalling IPv6
- Détecter et analyser les comportements malveillants à partir des flux et des logs
- Construire et exploiter un Security Lab IPv6 reproductible

Public visé

- Ingénieurs sécurité réseaux
- Ingénieurs réseaux
- Administrateurs réseaux et systèmes
- Analystes cybersécurité et SOC
- Architectes réseaux et sécurité
- Ingénieurs Cloud et infrastructure amenés à sécuriser des environnements IPv6

Pré-requis

- Bonne connaissance des fondamentaux TCP/IP, DNS et routage
- Compréhension de l'adressage et des principaux mécanismes d'IPv6
- Connaissances de base en sécurité réseau et firewalling
- Une pratique de Linux ou Windows en environnement réseau est recommandée

Pré-requis techniques

- Un ordinateur permettant d'utiliser les outils réseau nécessaires aux exercices
- Un navigateur récent et une connexion Internet stable
- Accès à l'environnement de laboratoire IPv6 fourni ou préparé pour la formation

Programme de notre formation Sécurité IPv6 : attaques, défense et ateliers pratiques

[Jour 1 - Matin]

Comprendre la surface d'attaque d'un réseau IPv6

- Identifier les différences de sécurité entre IPv4 et IPv6 et leurs conséquences sur les infrastructures
- Analyser l'adressage IPv6, les adresses link-local et les mécanismes d'autoconfiguration du point de vue de la sécurité
- Comprendre le rôle critique d'ICMPv6 et les risques d'un filtrage inadapté
- Analyser le fonctionnement de Neighbor Discovery Protocol (NDP), SLAAC, DAD et DHCPv6

- Identifier les risques supplémentaires introduits par les environnements dual-stack et les mécanismes de transition
- Atelier pratique : cartographier un réseau IPv6, capturer les échanges ICMPv6/NDP avec Wireshark et identifier sa surface d'attaque.

[Jour 1 - Après-midi]

Reconnaissance, spoofing et attaques Neighbor Discovery

- Mettre en œuvre les techniques de reconnaissance IPv6 et comprendre leurs différences avec les scans IPv4
- Analyser les attaques reposant sur les messages Neighbor Solicitation et Neighbor Advertisement
- Comprendre les scénarios de Rogue Router Advertisement et de détournement de trafic
- Identifier les risques liés aux faux serveurs DHCPv6 et aux configurations d'autoconfiguration non maîtrisées
- Étudier les scénarios de spoofing, flooding et déni de service affectant les mécanismes IPv6
- Mettre en œuvre les protections RA Guard et les contrôles de sécurité de niveau 2 adaptés
- Atelier pratique : reproduire un scénario Rogue RA dans un laboratoire isolé, observer ses effets puis configurer et valider les mécanismes de défense.

[Jour 2 - Matin]

Analyser les contournements et attaques réseau IPv6

- Comprendre les en-têtes d'extension IPv6 et leurs impacts sur les équipements de sécurité
- Analyser les risques liés à la fragmentation et aux chaînes d'en-têtes d'extension
- Identifier les possibilités de contournement des règles de filtrage et des équipements de détection
- Évaluer les risques associés aux tunnels et mécanismes de coexistence IPv4/IPv6
- Construire des règles de firewalling adaptées à IPv6 sans bloquer les fonctions essentielles d'ICMPv6
- Vérifier la cohérence des politiques de sécurité entre les piles IPv4 et IPv6
- Atelier pratique : analyser plusieurs flux IPv6 malveillants, identifier les techniques de contournement puis renforcer les règles de filtrage.

[Jour 2 - Après-midi]

Détecter et superviser les menaces IPv6

- Capturer et analyser les événements de sécurité IPv6 avec Wireshark et les outils réseau
- Configurer la journalisation nécessaire à la détection des comportements anormaux
- Exploiter les capacités IDS/IPS pour détecter les attaques et anomalies IPv6
- Identifier les équipements ou applications qui utilisent IPv6 à l'insu des équipes d'exploitation
- Construire des indicateurs permettant de superviser les flux et incidents IPv6
- Organiser l'analyse et la réponse à un incident affectant une infrastructure dual-stack
- Atelier pratique : détecter une activité IPv6 malveillante à partir de captures et de logs puis reconstituer le scénario d'attaque.

[Jour 3 - Matin]

Durcir une infrastructure IPv6

- Construire une stratégie de segmentation et de filtrage IPv6 adaptée aux usages de l'entreprise
- Durcir les mécanismes NDP, Router Advertisement, DHCPv6 et les équipements réseau
- Limiter les services, flux et mécanismes de transition inutiles
- Appliquer des politiques cohérentes aux environnements dual-stack
- Intégrer les contrôles IPv6 aux procédures de configuration, d'audit et de supervision existantes
- Tester régulièrement l'efficacité des protections et identifier les écarts de configuration
- Atelier pratique : auditer une infrastructure IPv6 volontairement mal configurée, appliquer les mesures de durcissement puis vérifier leur efficacité.

[Jour 3 - Après-midi]

Construire et exploiter un Security Lab IPv6

- Concevoir une architecture de laboratoire IPv6 isolée et reproductible
- Utiliser virtualisation et conteneurs pour reproduire différents scénarios réseau
- Construire un plan de tests associant reconnaissance, attaque, détection et mitigation
- Documenter les scénarios, résultats et preuves nécessaires à un audit de sécurité
- Définir une méthodologie de validation avant le déploiement d'IPv6 en production
- Construire une checklist de durcissement IPv6 réutilisable dans l'organisation
- Atelier pratique : conduire un scénario complet d'attaque contrôlée dans le Security Lab, détecter l'incident, appliquer les contre-mesures puis valider le durcissement.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.