

Comment protéger et sécuriser vos informations sur des réseaux TCP-IP : illustré de nombreux exemples pratiques et d'études de cas concrets, ce séminaire dresse l'état de l'art en la matière et répond à toutes les préoccupations actuelles dans le domaine de la sécurité TCP-IP.

- ITEM 1 : Identifier les types d'attaques sur les réseaux
- ITEM 2 : Savoir sécuriser les systèmes d'exploitation
- ITEM 3 : Définir la politique de sécurité : conception et mise en oeuvre
- ITEM 4 : Savoir isoler et protéger les réseaux TCP/IP
- ITEM 5 : Connaître la protection périmétrique par Firewall
- ITEM 6 : Savoir protéger les données de l'entreprise
- ITEM 7 : Déployer un VPN
- ITEM 8 : Paramétrer l'authentification des utilisateurs
- ITEM 9 : Savoir évaluer et faire l'audit de la sécurité
- ITEM 10 : Savoir sécuriser les services en ligne

Public ou prérequis **Les attaques sur les réseaux**

Avoir des connaissances de base sur TCP/IP et maîtriser un système d'exploitation.

Les origines des attaques et leur propagation
Evaluation du risque et applications à risque (DNS, HTTP, SMTP,...)

La sécurité des systèmes d'exploitation

La sécurité des différents systèmes : ITSEC, TCSEC, Unix,...
Les niveaux de sécurité D1, C1, C2, B1, B2, B3, A de l'Orange Book
L'exception Windows NT, les avis du CERT
Les authentifications Kerberos et LanMan

Activités principales

La politique de sécurité : conception et mise en oeuvre

Les objectifs d'une politique de sécurité globale, le rôle des hommes dans la sécurité
Externalisation de la sécurité ; concilier bon sens, technique et coût
Isolation et protection des réseaux TCP/IP
Les virus : typologie des attaques par le réseau, es serveurs anti-virus
Le plan d'adressage sécurisé, les serveurs proxy, le reverse proxy,...
Firewall ou proxy : concurrence ou complémentarité ?

La protection périmétrique par Firewall

Usages et pratiques du Firewall : le firewall le mieux adapté aux contraintes
Ressources nécessaires à l'administration et l'exploitation des firewalls
La détection des intrusions, les outils de remontée d'alertes et d'analyse de logs
Les solutions à haute disponibilité (Raware, legato, Stonesoft)
Le filtrage multi-zones et les données

La protection des données de l'entreprise

Fuite et vol d'information, violation d'intégrité, authentification des messages
Cryptage et clés de chiffrement

D
E
L
P
H
E
S

Ce programme est personnalisable et adaptable en fonction de vos besoins.

Tél. 04 94 16 90 70 www.delphes-france.net Fax. 04 94 16 90 77

Montrer l'enjeu que représente la sécurité sur les réseaux TCP/IP en dénombrant tout d'abord les problèmes existants liés à la sécurité, puis en étudiant les types d'attaques et finalement en proposant des solutions.

ITEM 1 : Les solutions pour isoler et protéger vos réseaux tcp/ip.

ITEM 2 : La protection périmétrique par firewall.

ITEM 3 : Comment protéger les données de l'entreprise.

ITEM 4 : Comment évaluer sa sécurité.

ITEM 5 : Sécuriser les services en ligne (facultatif)

ITEM 6 : Comment déployer un vpn.

ITEM 7 : Authentifier un utilisateur.

<p><u>Public ou prérequis</u></p> <p><i>Etre un utilisateur confirmé de l'internet et maîtriser un système d'exploitation.</i></p>	<p>Les virus : typologie des attaques par le réseau. Les firewalls dédiés / non dédiés ; où implémenter le ou les firewalls ? Comment se protéger des serveurs, des clients, de l'Internet. La mise en place de solutions DMZ (zones démilitarisées). Comment calculer le nombre de DMZ nécessaires. Les principales solutions du marché et leurs caractéristiques : Firewall-1 de Checkpoint, PIX de Cisco, M>Wall de Matranet, SecurWare de Bull.</p>	<p>D</p> <p>E</p>
<p><u>Activités principales</u></p> <p><i>Vous apprendrez à évaluer vos besoins et concevoir le système de sécurité le mieux adapté à ceux-ci en choisissant les solutions les plus efficaces parmi les offres du marché.</i></p>	<p>Comment sélectionner le firewall le mieux adapté à vos contraintes. Les firewalls : quelle exploitation au quotidien ? Quelle ressource nécessaire pour administrer et exploiter les firewalls ? Comment détecter les symptômes d'une intrusion. Les outils d'analyse de logs et de remontée d'alertes indispensables pour gagner du temps. Fuite ou vol d'information, violation d'intégrité, authentification des messages. Les algorithmes à clé symétrique / asymétrique. Comment crypter vos données avec DES, RSA, IDEA. Comment s'échanger les clés de chiffrement. Comment réaliser l'audit de la sécurité de votre réseau. Choisir entre audit une fois, répété ou permanent. Choisir les outils appropriés, les logiciels d'analyse de sécurité. Les logiciels de scan avancé ISS, Satan, Hoppa Scanner Port. Les détections temps réel (Real Secure, ...). La sécurisation des communications Web avec SSL et S-HTTP. Comment offrir un service sécurisé aux clients privilégiés. Dans quels cas le firewall est indispensable devant ses serveurs ? Les solutions DMZ sécurisées ; combien de DMZ ? Comment réaliser les mises à jour à distance et sécurisées. L'authentification renforcée, les vérifications d'intégrité. La création de VPN (Virtual Private Network) avec la solution firewall-réseau public-firewall. Comment déployer des accès distants à travers l'Internet. Les protocoles sécurisés L2F, L2TP, PPTP. Comment choisir entre VPN public et réseau privé opérateur Télécom. Mots de passe, token, carte à puce, certificats ou biométrie ? - Préserver la confidentialité des mots de passe. - Authentifier les accès entrants et sortants.</p>	<p>L</p> <p>P</p> <p>H</p> <p>E</p> <p>S</p>

Ce programme est personnalisable et adaptable en fonction de vos besoins.

Tél. 04 94 16 90 70 www.delphes-france.net Fax. 04 94 16 90 77

Comment protéger et sécuriser vos informations sur des réseaux TCP-IP : illustré de nombreux exemples pratiques et d'études de cas concrets, ce séminaire dresse l'état de l'art en la matière et répond à toutes les préoccupations actuelles dans le domaine de la sécurité TCP-IP.

- ITEM 1 : Identifier les types d'attaques sur les réseaux
- ITEM 2 : Savoir sécuriser les systèmes d'exploitation
- ITEM 3 : Définir la politique de sécurité : conception et mise en oeuvre
- ITEM 4 : Savoir isoler et protéger les réseaux TCP/IP
- ITEM 5 : Connaître la protection périmétrique par Firewall
- ITEM 6 : Savoir protéger les données de l'entreprise
- ITEM 7 : Déployer un VPN
- ITEM 8 : Paramétrer l'authentification des utilisateurs
- ITEM 9 : Savoir évaluer et faire l'audit de la sécurité
- ITEM 10 : Savoir sécuriser les services en ligne

Public ou prérequis **Les attaques sur les réseaux**

Avoir des connaissances de base sur TCP/IP et maîtriser un système d'exploitation.

Les origines des attaques et leur propagation
Evaluation du risque et applications à risque (DNS, HTTP, SMTP,...)

La sécurité des systèmes d'exploitation

La sécurité des différents systèmes : ITSEC, TCSEC, Unix,...
Les niveaux de sécurité D1, C1, C2, B1, B2, B3, A de l'Orange Book
L'exception Windows NT, les avis du CERT
Les authentifications Kerberos et LanMan

Activités principales

La politique de sécurité : conception et mise en oeuvre

Les objectifs d'une politique de sécurité globale, le rôle des hommes dans la sécurité
Externalisation de la sécurité ; concilier bon sens, technique et coût
Isolation et protection des réseaux TCP/IP
Les virus : typologie des attaques par le réseau, es serveurs anti-virus
Le plan d'adressage sécurisé, les serveurs proxy, le reverse proxy,...
Firewall ou proxy : concurrence ou complémentarité ?

La protection périmétrique par Firewall

Usages et pratiques du Firewall : le firewall le mieux adapté aux contraintes
Ressources nécessaires à l'administration et l'exploitation des firewalls
La détection des intrusions, les outils de remontée d'alertes et d'analyse de logs
Les solutions à haute disponibilité (Raware, legato, Stonesoft)
Le filtrage multi-zones et les données

La protection des données de l'entreprise

Fuite et vol d'information, violation d'intégrité, authentification des messages
Cryptage et clés de chiffrement

D
E
L
P
H
E
S

Ce programme est personnalisable et adaptable en fonction de vos besoins.

Tél. 04 94 16 90 70 www.delphes-france.net Fax. 04 94 16 90 77